2018
Help America Vote Act
Election Security Grants

Award Packet

April 17, 2018

U.S. ELECTION ASSISTANCE COMMISSION
1335 EAST-WEST HIGHWAY, SUITE 4300
SILVER SPRING, MD 20910

April 17, 2018

To: **Chief State Election Officers**
From: **Mark Abbott, Election Assistance Commission**
CC: **State Election Directors**
Re: **2018 HAVA Election Security Grants**

This award packet contains all the information you need to draw down your 2018 HAVA Election Security Grant funds. EAC is making the funds available for immediate access and use, subject to the contingencies found in the attached Notice of Grant Award (NGA).

To access the funds you will need to:

1. Make sure your Unique Entity Identifier (formerly DUNS) number and SAM (System of Award Management) account are accurate and up-to-date.
    A. Your Unique Entity Identifier (UEI) is issued by Dun and Bradstreet (D&B) www.dnb.com and consists of nine digits. EAC will need to verify that you are using the correct UEI before payment can be issued.
    B. Your SAM account must be renewed annually and must be active before a payment can be made. More information can be found at https://www.sam.gov/portal.

2. Send a letter via email from your Chief State Election Official to the EAC that includes the following information:
    A. The amount of funds you are requesting—you may request your entire award at one time or make a series of partial drawdowns during the five-year performance period of the award.
    B. Certification that, per Section 101(c)(1)&(2) of HAVA, funds will be used in a manner that is consistent with the laws described in Section 906 of HAVA and that funds will not be used in a manner that is inconsistent with the requirements of Title III of HAVA.
    C. Affirmation that you have reviewed and accept the terms of the award found in the Notice of Grant Award.
    D. A timeline and brief description of how you will develop the 1-3 page project narrative/budget for how the funds will be used in your state/territory. Note: The actual narrative submission and budget are due to EAC no later than July 16, 2018.
    E. Your UEI and the Certification Regarding Lobbying found at the end of this packet.

    Note that an optional Template for this request letter is provided at www.eac.gov/2018-hava-election-security-funds/

Special Notes on Funds

1. EAC encourages all States to immediately draw down or begin drawing down their funds. States have five years, until March 22, 2023, to draw down the funds, after which time the funds will automatically be returned to the U.S. Treasury.

2. Expenses can be incurred against the grant from March 23, 2018 onward. Contact EAC's grants office regarding reimbursement or matching credit for eligible expenses made prior to this date but after October 1, 2017.

3. Matching funds must be made available by March 23, 2020. Cash match must be deposited into the State Election Account. In-kind match must be tracked in the same manner as cash contributions. Both cash and in-kind contributions should be reported under Grantee Share on the annual Standard Form 425 Federal Financial Report (SF-425), which is due December 31 for the preceding October 1-September 30 period.

4. According to the Consolidated Appropriations Act, 2018 (Public Law 115-141), the purpose of this award is to "improve the administration of elections for Federal office, including to enhance election technology and make election security improvements". As such, using funds from this grant to pay for general operating expenses, historically paid for with non-federal funds, may not constitute an actual improvement to the administration of federal elections and may be questioned in a federal audit.

5. EAC will process all drawdown requests within 5 business days of receipt of the request.

6. EAC will hold a series of phone conferences and webinars over the summer to answer questions and support development of the required plans/budgets. Contact Mark Abbott at mabbott@EAC.gov with any questions you may have.

The following documents are included with this packet or can be found at the links below:

1. Notice of Grant Award
2. Submission Guidelines—Narrative and Budget
3. Required Federal Lobbying Certification
4. Budget Form at https://www.eac.gov/2018-hava-election-security-funds
5. FAQs at https://www.eac.gov/2018-hava-election-security-funds

2018 HAVA Election Security Grants
Program Narrative and Budget Submission Guidelines

Purpose. The purpose of the narrative statement and corresponding budget is to provide U.S. citizens, Congress, the EAC and other election stakeholders with information about how your state will use these funds to, as described in the Consolidated Appropriations Act of 2018 (P.L. 107-252), "improve the administration of elections for Federal office, including to enhance election technology and make election security improvements". States have express permission from EAC to pay for immediate election administration improvements ahead of the 2018 elections and prior to submission of this narrative and budget. This express permission applies only to non-construction expenditures.

The ninety-day period EAC is giving to States to develop this narrative and budget is designed to give you and your local voting jurisdictions time to assess your needs and develop robust plans to help secure voting systems and processes in upcoming elections. EAC will publish the narratives and accompanying budgets on its website. Information from annual state progress reports on implementing the activities described in the narratives/budgets will be consolidated and reported to Congress and the public by the EAC.

EAC encourages and will support states in developing high-quality submissions that reflect and highlight the important work you are doing to secure the vote in your state. States may use grant funds to host and/or participate in activities that can include, but are in no means limited to, the below activities as they develop their plans for using the funds:

1. Peer exchanges to share ideas and best practices
2. Coordination and collaboration with Department of Homeland Security (DHS), other federal- and state-level agencies and other groups with missions or activities related to cyber-security
3. Convening local and state listening sessions or hearings

EAC will hold forums and use its clearinghouse, website, and other forms of communication to highlight how states and localities are planning to use the funds.

Program Narrative Instructions. The narrative should be one- to three-pages in length and describe how your state or territory (hereon 'State') plans to spend the 2018 HAVA Elections Security Grant Funds and required matching funds. The narrative should include the amount of your award and matching commitment and the timeframe (up to 5 years) in which you plan to use the funds. The narrative should describe both immediate improvements/activities that are underway and/or that will be in place prior to the 2018 election and longer-term activities leading up to the 2020 election and beyond.

To ensure consistent reporting across states and localities, use the below categories when developing your narrative statement and corresponding budget. Use only the categories that are part of your planned activities and add to this list as needed. We will publish examples of state and local activities as they are shared with the EAC through these submissions.

1. Voting Equipment Replacement and Upgrades
2. Election Auditing
3. Voting Registration Systems and Management
4. Cyber Vulnerabilities
5. Training
6. Communication
7. Additional categories to be identified by States

Budget Narrative Instructions. The initial performance period for this award is five years, however you should submit a single budget that can be anywhere from 1 to 5 years in length depending on how quickly your state plans to spend the funds. For example, if your state will use the funds entirely on new equipment, the budget period would likely be only one year.
The budget you submit should be line item by category. An electronic version of the budget form can be downloaded at: https://www.eac.gov/2018-hava-election-security-funds. Budget categories include:

1. Personnel/Fringe Benefits
2. Equipment
3. Subgrants-Voting districts/counties
4. All Other Costs
5. Total Direct Costs
6. Indirect Costs
7. Training

The budget narrative should also include a breakdown by program category (e.g. Voting Equipment Replacement and Upgrades, Election Auditing, Cyber Vulnerabilities, etc.) and the approximate amount of funds that will be spent in each category. EAC will post a sample budget on its website to assist states in completing this portion of the application.

EAC Submission Review. Receipt of grant funds is not contingent on the content of each state's narrative/budget submission. However, EAC will review each submission and provide feedback and technical assistance that may require revisions to the narrative and budget submission. EAC will use the following review criteria:

1. Are the proposed expenses reasonable, allocable and allowable under HAVA and appropriate Office of Management and Budget (OMB) circulars?
2. Are the budget and program narratives sufficiently detailed to allow both stakeholders and federal auditors to understand the plan for spending the funds and track progress to know if the funds were used in an effective manner?
3. Are there activities or plans that could benefit from being informed by planned activities or experiences in another state?

EAC staff will offer feedback and technical assistance on each narrative/budget submitted.

To: US Election Assistance Commission

Certification Regarding Lobbying

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that: (1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement. (2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions.(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

NAME	TITLE	ORGANIZATION

SIGNATURE	DATE

ii) Recipient integrity and performance matters. If the total Federal share of the Federal award may include more than $500,000 over the period of performance, the Federal awarding agency must include the term and condition available in Appendix XII—Award Term and Condition for Recipient Integrity and Performance Matters. See also 2 C.F.R. §200.113 Mandatory disclosures.

2018 HAVA Election Security Grant

Notice of Grant Award

Grantee: State of New Hampshire

U.S. Election Assistance Commission
1335 East West Highway – Suite 4300
Silver Spring, MD 20910

Address:
State House, Room 204
Concord, NH 03301

Obligation Information

Agreement Number: **NH18101001**	Project Period: 03/23/2018 – 03/22/2023
CFDA Number: **90.404**	Budget Period(s): 03/23/2018 – 03/22/2023

Funds Description

This obligation of funds constitutes the Grantee's share of $380 million (*52 U.S.C. §§ 20901, 20903-20905*) authorized by the U.S. Congress under the *Consolidated Appropriations Act, 2018 (Public Law 115-141).*

Funding Information

Description	Current Award (Obligation) 2018	Prior Awards N/A	Cumulative Funding
Federal Share	$3,102,253	N/A	$3,102,253
State Match Share (5%)	$155,113	N/A	$155,113

Purpose

As authorized under Section 101 of the Help America Vote Act of 2002 (P.L. 107-252) (HAVA) and provided for in the Consolidated Appropriations Act, 2018 (Public Law 115-141), the purpose of this award is to "improve the administration of elections for Federal office, including to enhance election technology and make election security improvements" to the systems, equipment and processes used in federal elections.

State Election Fund

All Federal funds and state cash matching funds must be deposited in the state election fund as described in Section 104 (d) of HAVA. Cash and in-kind match expenditures require the same documentation as federal funds under 2 C.F.R. § 200. Interest earned on this award's funds and any net program income shall be retained in the election fund and used for allowable activities described in Section 101 of HAVA.

Grant Administration

Award recipients and sub-recipients must adhere to all applicable federal requirements including Office of Management and Budget (OMB) guidance: Title 2 C.F.R. Subtitle A, Chapter II, Part 200-Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 C.F.R. § 200).

Reporting Requirements

Per 2 C.F.R. § 200, program narrative and expenditure reports (Federal Financial Report SF-425) are due by December 31 for the preceding October 1st to September 30th period. Narrative reports must include a summary of expenditures aligned with budget categories in the grantee's plan, a list of equipment obtained with the funds, and a description of how the funded activities met the goals of the plan.

Award Contingencies

This award is contingent upon the completion of the following activities:
1. Provide a match of 5% of the Federal funds within 2 years of this award to be documented on the annual SF-425 submission.
2. Submission of the required documents included in the 2018 HAVA Security Grant Awards packet attached to this Award Notice within 90 days of the date of this award.
3. Implement or have implemented the Drug-Free Workplace Requirements of 2 C.F.R. § 182.200 and comply with subpart C of 2 C.F.R. Part 180- Debarment & Suspension & include in lower-tier covered transactions.

Acknowledgement

By drawing down funds under this grant, the State agrees to comply with all terms and conditions in this Notice.

U.S. Election Assistance Commission	**Funding Source: EAC18-1908NH**
Signature: BDN	**Amount: $3,102,253**
Brian D. Newby, Executive Director Date April 17, 2018	

ANDERSON
ECONOMIC
GROUP

April 30, 2018

Mr. William M. Gardner
Secretary of State
N.H. Department of State
State House, Room 204
107 North Main Street
Concord, NH 03301-4989

RE: Election Forensics Consulting Services

Dear Mr. Gardner:

I am writing you to inform you of an exciting new service offering from Anderson Economic Group. We now provide election forensics services that assist agencies like yours to ensure fair and secure elections in New Hampshire and to deter attempts at tampering and fraud.

Anderson Economic Group pioneered a number of election forensics methods, and demonstrated them in real time in the days immediately following the 2016 Presidential election. We have made use of lessons learned in our work with election data in Michigan, Pennsylvania, Wisconsin, and California in outlining the election forensics services we are now prepared to offer you and other election officials.

Benefits of Election Forensics Services

There are clear benefits to these services, including:

- The ability to identify significant anomalies within specific regions, which may indicate fraud, hacking, mistakes, or other potential sources of anomalous results.
- Deterrence of organized efforts to hack into election data, government systems, and related software and hardware, by significantly increasing the chances that such efforts would be identified quickly.
- Reduced need for expensive and time-consuming recounts and audits of a large number of districts, when a focused effort involving specific districts would be less expensive and more likely to confirm the existence or absence of significant irregularities.
- A published methodology, used by an independent party with a track record of accurately assessing election results in multiple states immediately after the 2016 election.
- Enhanced public confidence in election results.

Our Track Record

Immediately after the November 2016 Presidential election, a number of computer scientists, activists, political candidates, and competing political factions asserted that fraud and tampering had occurred in certain states, including Michigan, Wisconsin, and Pennsylvania. Expensive recalls were undertaken in at least three states, and subsequent audits as well. A US government report at that time asserted that Russian interference had occurred, but did not assert tampering with election tallies.

We conducted county-by-county election forensics analyses in December 2016 and January 2017 in Michigan, Wisconsin, Pennsylvania, and California. Our results and a summary of methodology were published at that time. Our findings, based on that methodology, included:

- No evidence of systematic tampering, hacking, or changes in vote tallies in Michigan, Wisconsin, or Pennsylvania.
- Unusual voting patterns in a small number of counties, which we stated merited further inspection but did not prove fraud had occurred. In one such county, a subsequent investigation and audit demonstrated widespread irregularities among precincts, which was attributed to widespread human error.
- No evidence of systematic voting by immigrant populations without citizenship in Michigan, Wisconsin, or Pennsylvania.
- An inability to determine, from the aggregated county data available at that time, any findings within California. We identified then that disaggregated data would be necessary for this very large population state for reliable use of this methodology.

These analyses proved quite accurate. Subsequent reports indicate that Russia attempted to hack into the election systems of 21 states, succeeding to some extent in seven of those states. However, no evidence has yet been found of systematic effects on vote tallies in any of the states we analyzed. Furthermore, no evidence has yet been found of systematic illegal voting of immigrants without citizenship in the three states for which we were able to assess the evidence. Aside from the irregularities found in one county (which was identified in our analysis as unusual), no evidence of widespread irregularities or organized fraud was confirmed in any of the three states for which we had the data necessary to complete our analysis.

Our Suggested Plan of Work

We have outlined, based on our experience and our previously-published results and methodology, a recommended plan of work for states, cities and counties interested in deterring election tampering and enhancing voter confidence. That plan of work includes:

1. Working closely with you to collect relevant data on the voting behavior of residents in past elections, by specific counties, precincts, or districts, in the months leading up to Election Day.
2. Analyzing these data to establish the historic statistical patterns among districts, for specific types of elections.
3. Presenting to you a protocol for the assessment of the forthcoming election, including the specific methods to be used, timeline, format for reporting, and description of possible results. This protocol

can be prepared in a manner that can be published in advance of the election, and is explicit about the purpose of the analyses, the types of activities that can be detected and those that cannot, and the meaning of words and phrases that could be applied to future results.

4. Quickly analyzing the results after the election, on a timeline reviewed with you in advance. Using the protocol previously outlined, we will attempt to detect whether there is evidence of significant anomalies that could indicate fraud or tampering.
5. Preparing a draft report and answering questions regarding the data, findings, and methodology on a timeline reviewed with you in advance.
6. Formalizing our findings and communicate them to you, in the format previously identified.

Our methods are non-invasive; do not involve any interference with voting or canvassing; protect voter anonymity; and respect the limited availability of resources and time at government agencies, including during and immediately after Election Day. In addition, our statistical techniques focus on patterns of voting demonstrated by the voters themselves, and not any recommendation, polling, or social science model of that voting. Finally, while our findings will provide you and others ~~with~~ valuable information, they will not substitute for the statutory process of canvassing and certifying elections.

Conclusion

We understand that you are committed to the integrity of our election system, and we believe that election forensics can be an essential tool to instill confidence in the security of the democratic process. If you have any questions or would like to discuss Anderson Economic Group's election forensics capabilities further, please call me at (517) 333-6984. We would be happy to provide a presentation with further details, upon request.

Sincerely,

Jason Horwitz
Director, Public Policy and Economic Analysis

CC: Robert P. Ambrose, Senior Deputy Secretary of State

Center for American Progress
State Election Security Preparedness
February 12, 2018

There are a number of legitimate concerns raise by this study. We in New Hampshire are concerned, however, with the implicit pressure to follow the federal lead and seek the lowest common denominator in implementing election technology, an approach that has often failed in the past.

New Hampshire has adopted many best practices in implementing cybersecurity requirements for its voter registration database and in training local officials. Because New Hampshire has election day registration, no qualified person will be unable to vote if their name does not appear on the checklist. The state also has well-known and widely circulated methods to count ballots manually, in the event this becomes necessary.

There are a number of shortcomings in the analysis:

1. **Federal intervention.** Many states got into trouble after the passage of HAVA in 2002, following the leadership of the newly-established U.S. Election Assistance Commission, that encouraged them with funding and provided certification, enabling states to get rid of paper trails when counting ballots, eliminating the possibility of both recounts and audits. This situation remains an open problem nationally. New Hampshire did not follow the federal lead and retained a much more credible election counting process. What is the credibility of federal cybersecurity in light of the recent past? CAP's study argues for enlisting help of federal authorities. We have seen that a feral agency, in this case the EAC, will be under pressure to yield to certifying the lowest common denominator. The state should not be pressured to buy something that only passes the lowest common denominator test, which is the federal test.

2. **Disclosure of information technology architecture and protocols**. Why would states give away their election software architecture and protocols and effectively advise their adversaries what, if any, vulnerabilities they should target? CAP scored New Hampshire down for following a best practice of not disclosing architecture and protocols.

3. Electronic poll books without high standards. Given existing standards in most states except New Hampshire, electronic poll books can be implemented that would, in the event of an e pollbooks failure on election day, leave local election officials with a blank paper checklist.

Election officials would not know who had voted before an electronic poll books system failed. In light of electronic poll books failures in 2012, 2014, and 2016, New Hampshire requires that electronic poll books be able to print out a marked checklist (showing who had cast ballots up until the moment of failure) in the event electronic poll books fail on election day. This is a reasonable security protection that New Hampshire is holding out for before it implements electronic poll books. The CAP study calls for electronic poll book testing and the availability of back-up voter registration lists in event of failure. Based on CAP's criteria, New Hampshire should receive high grades.

4. **Reliance on incomplete federal voting system standards.** New Hampshire has more demanding standards and expectations of voting systems than what is on the market and can be verified. CAP recommends the states go out and purchase, simply on the basis of incomplete federal certification standards, new equipment that has not been proven in as many recounts and has passed as many tests as New Hampshire's system has. New Hampshire was scored down for adhering to higher standards than the federal voting system standards.

5. Air gaps. An air gap is a network security measure employed to ensure that a secure computer network is physically isolated from unsecured networks. Normally air gaps are considered effective in avoiding hacking and interference, because they make it harder for hackers to infiltrate. New Hampshire's State Police drive hard copies of the election night results to the Secretary of State on election night, so there is a sort of enforced accountability at the local level, where ballots are counted and results are announced and normally posted transparently. Instead, CAP appears to recommend electronic transmission to a central server, which entails fewer air gaps and arguably less transparency in election night reporting. New Hampshire already is well known for its demanding reconciliation requirements at both local and state levels.

6. one4all, an open sources accessible voting system. With the help of Professor Juan Gilbert and his team at the University of Florida, New Hampshire has become the first state in the country to roll out and use an open source accessible voting system statewide in three different types of elections, Presidential Primary, State Primary and General Election. These elections each entail quite different ballot design and requirements. Relying on user input from the New Hampshire disability community, the Secretary of State has implemented three major voice upgrades in the last year, and has successfully marked a pre-printed ballot, the gold standard that helps assure voter privacy. No other state has attempted so ambitious a project in house. No other state actually re-designs its own user interface in every election.

Now that New Hampshire has achieved this goal, we are more likely than other states to want to plan the steps of designing a vote tallying device, and to resist pressure to purchase the latest vote counting device with a lot of bells and whistles, relying substantially on the lowest common denominator established by the federal EAC, as suggested by CAP.

7. Paper reliance in New Hampshire... Best practice sin training hand counting of paper ballots.

8. Electronic poll books. New Hampshire received a "Fair" from CAP, when it has produced the latest set of best practices and requirements, standing on the shoulders of Indiana, Virginia and Connecticut.

Version 1.0
February 2018

Center for Internet Security®

A Handbook for

Elections Infrastructure Security

002973

Center for Internet Security®

About CIS

CIS is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities.

Center for Internet Security®

31 Tech Valley Drive
East Greenbush, New York 12061

T: 518.266.3460
F: 518.266.2085
www.cisecurity.org

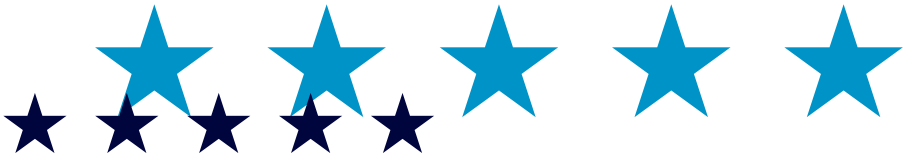
Follow us on Twitter @CISecurity

002974

Version 1.0
February 2018

A Handbook for

Elections Infrastructure Security



https://www.cisecurity.org/elections-resources/

Acknowledgments

CIS would like to recognize the following individuals and organizations for their support in creating this handbook. Their time and expertise were invaluable in completing this important work.

CIS authors

Brian Calkin
Kelvin Coleman
Brian de Vallance
Thomas Duffy
Curtis Dukes
Mike Garcia
John Gilligan
Paul Harrington
Caroline Hymel
Philippe Langlois
Adam Montville
Tony Sager
Ben Spear
Roisin Suver

Community contributions to and review of the handbook

Joseph Lorenzo Hall
Center for Democracy and Technology

Noah Praetz
Cook County, Illinois

Adam Ambrogi
Democracy Fund

Mike Goetz
Election Systems and Software

Tim Mattice
The Elections Center

Peter Lichtenheld
Hart InterCivic

Yejin Cooke
National Association of State CIOs

Susan Frederick and Danielle Dean
National Conference of State Legislators

Tim Blute and David Forscey
National Governors Association

Joshua Franklin and Gema Howell
National Institute of Standards and Technology

Emefa Agawu and Ian Wallace
New America Foundation

Tony Adams
Secure Works

Daniel Kambic and Greg Shannon
Software Engineering Institute

Trevor Timmons
State of Colorado

Robert Giles and Kevin Kearns
State of New Jersey

Tom Connolly
State of New York

U.S. Department of Homeland Security

Ryan Macias and Matt Masterson
U.S. Election Assistance Commission

David Mussington
University of Maryland

J. Alex Halderman
University of Michigan

Marian Schneider
Verified Voting

Contributions of current best practices
In addition, we'd like to thank the following individuals and organizations for providing examples of best practices in use today.

Beth Dlug
Allen County, Indiana

Emmit Lamb
Clark County, Nevada

Chris Chambliss
Clay County, Florida

Scott Konopasek
Contra Costa County, California

Kyle Rulli
Douglas County, Colorado

Stan Bethea
Duval County, Florida

Mark Earley
Leon County, Florida

Joe Miller
Linn County, Iowa

Bill Burgess
Marion County, Oregon

Faith Lyon
Portage County, Ohio

Ricky Hatch
Weber County, Utah

Part 1: **Introduction**

How cybersecurity and elections intersect and why it matters.

To enable the elections that define democracy, we must protect the security and reliability of elections infrastructure. Through a best practices approach, we aim to help organizations involved in elections better understand what to focus on, know how to prioritize and parse the enormous amount of guidance available on protecting information technology (IT) systems, and engage in additional collaboration to address common threats to this critical aspect of democracy.

The Center for Internet Security (CIS) and its partners publish this handbook as part of a comprehensive, nationwide approach to protect the democratic institution of voting. Election officials have been working diligently to secure their systems but, like so many other sectors, the threat to national security rises above any individual organization; we can accomplish more together, and we all share the same goal of free and fair elections. To that end, CIS is committed to a long-term effort to continuously advance and promote best practices for elections security as part of a national response to threats against elections infrastructure. This handbook addresses cybersecurity-related aspects of elections systems.

Background and purpose

Elections are the bedrock of democracy. Even before the establishment of the United States, adversaries sought to corrupt, interrupt, or otherwise disrupt democracy by subverting elections. From adversarial nation states, to terror groups, to Boss Tweed vote strikers, to those simply wishing to wreak havoc, attacks on the voting process are as old as voting itself. There is no way around it: protecting democracy calls for protecting elections.

The desire of some to disrupt elections has not changed; Joseph Harris's 1934 seminal book on elections, *Election Administration in the United States,* enumerates a series of election fraud incidents throughout American history. What is different in recent years is some of the tactics of such efforts to undermine democracy. Attacks leveraging weaknesses in digital infrastructure now augment traditional approaches and have become an increasingly common approach.

Judging by activity in industries and sectors outside elections, this should come as no surprise. Organizations across all sectors and government entities alike face daily attacks from actors with widely varying levels of sophistication. The most capable, best protected organizations have specific plans for addressing evolving threats. The plans are never static; these entities continually adapt—as do their adversaries—requiring an ongoing investment in security.

Moreover, in many industries and sectors, the good guys have realized that a go-it-alone strategy isn't enough. They've developed approaches that allow them to share information, establish best practices, and develop coordinated response plans to mitigate effects of coordinated attacks. This collaboration raises the level of security for the individual organizations, their respective industries or sectors, and the country.

Even in the financial services industry—in which annual investments by individual organizations in improved security for their digital systems can range in the many hundreds of millions of dollars—organizations pool some resources to support the Financial Services Information Sharing and Analysis Center. This collaborative approach to monitoring the evolving threat environment helps support even the most substantial individual efforts. These same approaches have been repeated in many industries, including communications, the defense industrial base, aviation, oil and gas, real estate, electricity, and others. Protecting elections infrastructure is certainly no less important to our country's national security and overall well-being than protecting the infrastructures in these other vital sectors.

In the state and local sector, the Multi-State Information Sharing & Analysis Center (MS-ISAC) works with state and local entities to monitor threats to their systems, detect common attacks across states, and support mitigation of risks presented by vulnerabilities and changing attacker behavior. This results in a more rapid deployment of solutions when new threats emerge; if there's one thing we know about these actors, once they succeed in an attack, they'll duplicate it everywhere they can.

The parent organization of the MS-ISAC and sponsor of this handbook, CIS, has used collaboration among a large number of security experts as a means to identify best security practices. These collaborative processes have resulted in several products available to state and local governments and other entities, including election officials and their technical staff. These include the CIS Controls and CIS Benchmarks, which heavily inform the recommendations in this handbook.

An underlying reality to all current work in cybersecurity is that a skills gap exists for cybersecurity globally, across all industries—elections included. Closing this skills gap is critical to elections and securing the process. Implementing best practices is only possible with the right people who have the necessary skill-set. Therefore, we hope what follows in this handbook will serve individuals with differing skills and resources in implementing practical guidance for election administration.

The elections environment

Elections in the United States are highly decentralized with more than 8,000 jurisdictions across the country responsible for the administration of elections. While the federal government provides some laws and regulations, states have substantial discretion on the process of conducting elections. The federal government does not administer elections and has a limited role in dictating how the process is to be conducted.

States act as the primary authority for the laws and regulations that govern the process of conducting an election in that state. Under federal law, states must designate a chief state election official. This official typically sets rules and regulations for the implementation of election technologies and their use. Although states are heavily involved in setting the rules and policies for administering elections, and in choosing election technology, in most states local jurisdictions administer and conduct the processes of an election.

Many local jurisdictions have the ability to procure their own election technology from a set of certified or approved manufacturers and vendors designated by their respective state. Additionally, the local jurisdictions are typically responsible for inventorying, securing, and training staff on those technologies. Depending on the size and resources of the jurisdiction, the number and technical skills of the staff can vary greatly, ranging from an elections team with its own dedicated IT and security personnel to a single person with little to no IT background. Many elections offices rely on IT resources shared with other administrative functions (e.g., other county agencies) or rely exclusively on technology providers (e.g., elections and IT systems vendors) for implementing and securing their election infrastructure. This can result in dependencies that are outside of the local officials' control.

Audience

By using this handbook, we hope election officials and those that manufacture, own, operate, or are otherwise involved with elections systems and their IT components are better able to understand and prioritize risks, understand best practices that can identify threats, detect attacks, allow for recovery from cybersecurity incidents, and, ultimately, continue to provide and support systems for the execution of free and fair elections.

In addition to this handbook providing a path to continually evolving security, perhaps the most important aspect of this effort is to help instill a continued sense of faith in elections by voters themselves. We hope election officials are able to use this handbook to highlight the past and ongoing work they've done to secure the elections process and that, through openness, transparency, inclusion of relevant stakeholders, and consideration of the entirety of the elections process, voters recognize that democracy is working and their votes will count.

More specifically, we hope this handbook is of use to each of the following:

- **Election officials and senior executives.** These individuals are accountable for executing elections. In addition to state and local election officials, they may include those indirectly involved in the election process, such as the offices of legislators and governors.
- **Owners and operators of elections systems.** These individuals have more responsibility for the systems themselves, though there may be some overlap with election officials. It's critical that they understand the risk context and the technical guidance in this handbook.
- **Vendors of hardware and software.** Whether providing systems and services dedicated to elections or general purpose but used in elections, vendors are, and must remain, partners in this process. Moreover, vendors often provide the primary technology expertise and labor to local election officials. Vendors have a vested interest in their products and services, and election officials driving vendors toward best practices can help all boats to rise with the tide, including improvements in the development, testing, and continual evolution of vendors' products.
- **Others who can help secure elections.** This includes the U.S. Election Assistance Commission. (EAC), the U.S. Department of Homeland Security (DHS), state chief information officers and chief information security officers, state homeland security advisors, fusion centers, election integrity groups, academics, and other non-profits and private companies willing to lead or support various efforts. This is, in many ways, a baselining effort that we hope supports other efforts dedicated to improving the security of elections, both new and ongoing.
- **Voters, the media, and other interested stakeholders.** In the end, no stakeholder matters more than voters. Not only is it the duty of all to ensure elections represent the will of voters, but it is the duty of all to ensure that voters have confidence in the process before heading to the polls and after results come in.

Goals and outcomes

This handbook is about establishing a consistent, widely agreed-upon set of best practices for the security of systems infrastructure that supports elections. It provides both a general explanation of the threats that exist for the various components of the elections process and examples of known mitigations for these threats.

By developing and publishing this handbook, CIS aims to establish a baseline of protection for all aspects of the elections infrastructure ecosystem that leverage digital tools and applications. The primary goal of this handbook is to impact and improve the security of elections infrastructure as soon as possible, and ideally in advance of the 2018 elections, and establish a set of best practices that, with continual updates, supports elections infrastructure security into the future. We expect many elections systems will already incorporate the majority of these mitigations, allowing those jurisdictions to demonstrate a strong baseline. In that case, the handbook can assist in prioritizing for continual improvement and evolution.

Handbook structure

This handbook is divided into three parts that together provide a baseline view of how to manage cybersecurity risk in elections:

- **Part 1: Introduction.** This introductory section describes this handbook and provides some general information on risk assessments in elections systems.
- **Part 2: Elections Systems and Risk**. The second part **introduces a high-level generic elections architecture,** some components of which may exist at the state level, some at the local level, some both, and some not applicable in certain jurisdictions. It also **classifies these common components of elections systems according to the manner in which they are connected to networks or other systems.** For each major component of the generic elections infrastructure, there is an overview and description of how it fits in the elections landscape and a brief description of the risks and threats associated with the component. Finally, it summarizes the classification-based ways that different implementations of the components are connected to other digital infrastructure.
- **Part 3: Mitigating System Risk.** The third part is a **technical best practice guide that provides controls and recommendations for systems.** It includes two major sections: 1) a set of critical risk-mitigating activities that can benefit any organization and 2) a set of technical best practices for users, devices, software, and processes that are listed first for components that are network connected and then for those that are indirectly connected. We also provide technical best practices that address transmission of information among digital components of the elections infrastructure. As described below, the nature of the connectivity to other elements of the elections digital infrastructure is the major security vulnerability area and thus we have chosen this connectivity as the basis for organizing technical controls. Technical staff, whether government or contracted resources, should be able to implement these controls to provide an appropriate mitigation of risk.

What this handbook is not

A shortcoming of many efforts in domains as large as IT security and elections is a failure to properly scope efforts. In addition to describing what this handbook is, we want to be explicit about what this handbook is not.

Aspects of elections, voting, and protecting democratic institutions that are not part of the scope of this handbook are not an indication of importance, but rather an acknowledgment that no single effort can successfully address everything. This handbook limits its scope to only digital aspects of elections themselves, though in some cases it references paper-based processes in order to further the discussion. The one exception to this is the recognition of how the means of transmission can inject cybersecurity risks, such as digitally transmitting to-be-paper pollbooks to a printer. In these cases, we identify the transmission risks in Part 2 and the mitigations to transmission risks in Part 3.

Beyond this, there are several aspects of election security we do not address. This handbook is not:

- **A one-size-fits-all.** This handbook **does not recommend any single approach to managing election systems or developing and deploying elections systems technology.** Election jurisdictions tailor their voting processes and systems to the needs of their voters and jurisdictional laws and requirements. That said, there are many commonalities. Rather than focus on differences of approach, this handbook focuses on the best practices associated with common approaches, recognizing the variety of approaches and architectures wherever possible.
- **An all-encompassing scope.** As this handbook is about improving the security of elections infrastructure as it exists today, **we have intentionally left several aspects of the broader voting process, however important, out of scope:**
  - Eligibility for an individual to register to vote;
  - Voter identity verification, unless specifically about the accuracy and availability of voter registration rolls;
  - Security of campaigns or campaign information systems; and
  - The accuracy of information about candidates or issues, including those conveyed using social media.

Assessing risk in elections systems

A common way of describing an organization's cybersecurity posture is in terms of risks that have been mitigated and risks that have been accepted. Those outside the information security community will often think of security in terms of stopping all possible threats. Both within the community and in the legal domain, practitioners understand that perfect cybersecurity is not possible. Rather, organizations seek to achieve "reasonable" security that involves accepting some level of risk given the threats and potential consequences, while maintaining an ability to recover should any of those consequences be felt.

Elections systems risk overview

The IT systems infrastructure that supports our elections processes has myriad risks, and these risks vary from one organization to the next. There are a number of commonly used risk assessment approaches that can be used by election officials and their technical staff to help assess risk, such as International Organization for Standardization (ISO/IEC) 27005 and National Institute of Standards and Technology (NIST) Special Publication 800-30. Among the most popular tools for understanding and managing cybersecurity risk is the NIST Cybersecurity Framework, which organizes cybersecurity activities in five functions: identify, protect, detect, respond, and recover.

Unfortunately, many election officials do not have the expertise or resources to conduct an adequate risk assessment. The ability to efficiently and effectively execute a risk assessment is further reduced by the difficulty in objectively assessing evolving threats, as well as the complexity of the elections processes and systems.

In its simplest form, a risk assessment is used to identify and assess the impact of vulnerabilities—weaknesses that an attacker can exploit—while being mindful of the compensating controls that exist in a system. These risks can be mitigated with appropriate physical, process, and technical safeguards. In this way, risk and potential impacts can be reduced to a level deemed acceptable by the accountable election officials, often called a balanced risk posture. The potential impact or consequence of a successful exploit is an important part of a risk assessment as elections officials want to focus first on exploits that have the greatest potential consequence.

While some risks vary from one election jurisdiction to another, many are common across the wide variety of elections systems configurations. As part of producing this handbook, experts have collaborated to assess the common risks to elections systems. This common baseline risk assessment has influenced the prioritization of security best practices in the handbook.

Baseline elections risk assessment

The baseline assessment of risk for elections is summarized for the purpose of helping election officials and their technical staffs understand the major areas of risk that can serve as their primary focus. Each organization should augment the baseline elections risk assessment to address the risks that might be unique to their elections processes, systems, and threats.

A top-level assessment of vulnerabilities and potential consequences to the elections systems infrastructure identifies network connectivity—devices or systems that work with other devices or systems to achieve their objectives—as the major potential vulnerability. The reason is simple: given an adversary with sufficient time and resources, systems that can be accessed via a network cannot be fully protected against compromise. There are ways to improve the security of network connected systems with additional controls, but the inherent complexity of network connectivity results in significant residual vulnerabilities.

Therefore, risks for system components that are connected to a network should be treated differently than for components that are never connected to a network. In this handbook, the definition of "network" includes connections to the internet as well as connections to both local wired and wireless networks.

While systems that are continuously connected to a network have a somewhat higher risk than systems that are only intermittently connected to a network, experts have demonstrated that any network connectivity, even if only for a limited period of time, results in a significantly larger vulnerability profile. An access path to these components may be available through the internet if any connected component can access the internet, and thus an attack can be orchestrated from anywhere in the world. The box to the right illustrates examples of these threats.

On the other hand, systems that have a digital component but are not network connected have a reduced vulnerability profile. Specifically, there are fewer ways to attack such systems and devices, but it does not mean the consequences of a successful attack are any lower—indeed, an attack can still be executed without geographic boundaries. The methods used to upload and download information (e.g., USB sticks, memory cards) still have vulnerabilities, but there are fewer vectors of attack to mitigate.

Examples of threats and consequences

Scenario 1:
A nation-state uses the internet to access and disrupt one or more state voter registration databases such that legitimately registered voters are denied the ability to vote on election day, or are required to file a provisional ballot.

Consequence:
Although no votes are manipulated, this attack would likely be a major national news story that results in reduced confidence by the public in the integrity of the voting process and the election results. Additionally, this slows the voting process, creating the risk of long lines and making in-person voting less efficient.

Scenario 2:
An adversary gains access through the internet to one or more election night vote displays and changes the displayed results such that the real winner of the election is now the reported loser in the election.

Consequence:
Again, while no votes have been changed, and the erroneous posting of election results by an authoritative source will subsequently be republished correctly, there is likely to be a significant loss of voter confidence.

Three classes of elections systems

In this handbook, we have organized best practices into two classes based on the different threat characteristics associated with levels of connectedness. A third class, that of processes that are executed without a digital component, such as hand-counted paper ballots—the casting and counting of ballots via purely paper and manual means—is out of scope for the handbook.

While there are many components to a complete election system, many of the cybersecurity risks associated with them can be grouped to simplify the steps to manage risk. One approach to this is by analyzing the manner in which they connect to networks and other devices. Throughout this handbook, we classify components of elections systems based on three types of connections that most clearly define the risk landscape:

1. **Network connected systems and components.** Network connected components are interconnected with other devices to achieve their objectives. The level of interconnection, while providing various benefits, also introduces additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means for accessing and managing the devices, which means organizations must make extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet, nor does their connection have to be persistent. As an example, an Election Management System (EMS) connected to a private county network would still be classified as a network connected system.

2. **Indirectly connected systems.** Indirectly connected components are not connected to a network at any time and are not persistently connected to other devices. They do, however, have to exchange information with other elections system components including network connected systems in order to complete their objectives in the election process. These information exchanges are done using removable media such as USB drives or other flash media. While the risks associated with being connected to a network or the internet are no longer relevant, threats are introduced by exchanging information with other devices, either through the use of removable media or a direct connection to another device such as a printer or an external disk drive.

3. **Non-digital elections components.** These are aspects of the elections process that have no digital component and are **out of scope for this handbook.** An example would be the mailing, completing, and returning of a paper mail-in ballot. While aspects of the overall process—such as an online request for the ballot—may leverage digital infrastructure, the aspect of this process that is purely paper-based is out of scope.

In Part 2 of the handbook, each major component of an election system is briefly described and then placed into one of these classes, providing a method to simplify the risk landscape and assist officials and their technical staff in determining the most effective and efficient approaches to managing risk. In some cases, major components are divided into the primary approaches to executing a process, such as the different approaches to conducting vote capture, each of which is classified individually. This classification analysis becomes the foundational basis for an elections organization selecting the appropriate technical best practices for that component described in Part 3 of the handbook.

Transmission between components creates vulnerabilities

While securing elections systems components is important, one of the largest sources of vulnerabilities, and thus most common methods of attack—attack vectors in cybersecurity parlance—lies not in the systems but in the transmission of data between systems. Weaknesses in communications protocols, or in their implementation, risk exposure or corruption of data, even for systems that are otherwise not network connected. For instance, while paper pollbooks wouldn't typically have cybersecurity risks, if the data for the pollbooks is sent electronically to a printing service, this transmission introduces risks that must be addressed. Similar vulnerabilities exist in transmission of ballot layout information to printers or in loading ballot information into ballot scanning (i.e., vote capture) devices. In Part 3, we also address transmission risks of this nature and the best practices that can mitigate them.

Part 2: **Elections Systems and Risk**

A description of major elections components and their risks.

This part of the handbook provides a generalized elections systems architecture showing each major component of the systems and:

1. A discussion of the risks and threats for each major component,
2. For some components, a description of the different types of deployment in use, and
3. A classification of the component based on how it connects to other devices, and thereby a mapping to controls and recommendations in Part 3 of this handbook.

A generalized elections systems architecture

There are many flavors of elections infrastructure, both from a technology and a process perspective. This is true far beyond just the different types of vote capture and vote tabulation devices. That said, many experts have studied the elections process at length, and there are several fundamental components common to nearly all elections systems.

In some jurisdictions, the owner of various aspects of the architecture may differ, but the fundamentals of the types of systems used to perform the task are generally the same. For that reason, many of the best practices associated with those systems will closely follow IT security best practices. Those accountable for elections infrastructure should understand these basic processes and identify the parts where they have purview. A description of major system components that comprise the elections infrastructure are shown in [FIGURE 1].

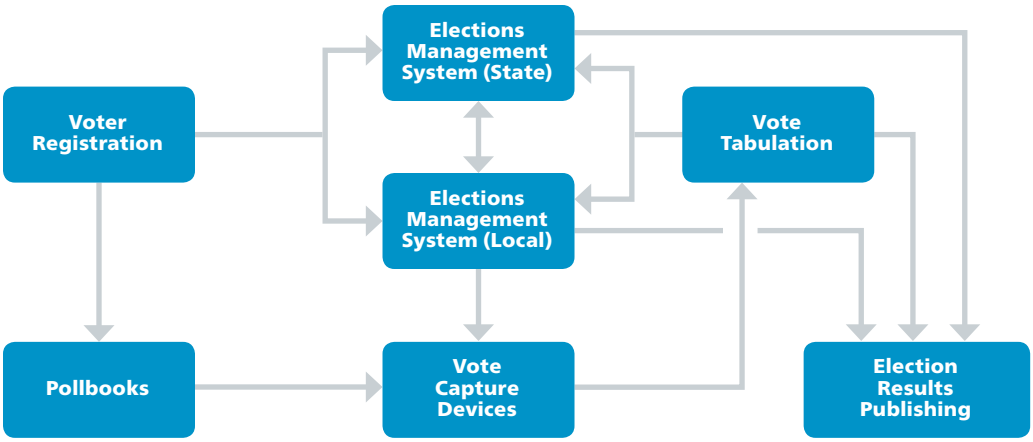


FIGURE 1: *A generalized elections systems architecture*

While each of these systems has IT components that require security best practices, this handbook addresses a subset that are, in our view, the highest risk targets of attack by adversaries and thus require the bulk of the attention. For digital components not covered in the handbook, the analysis methods used here can be applied to determine the appropriate set of technical best practices for that component.

Many of the components in elections infrastructure are built on general purpose computing machines, such as traditional web servers and database platforms. While this means they are often subject to the same attacks as those in other sectors, it also means experts have identified best practices to mitigate many of the risks.

Each of these components may exist at the state level, at the local level, or both, and some will not be applicable in certain jurisdictions. Nonetheless, all will exist in most jurisdictions and must be addressed in order to provide a comprehensive best practices guide. This is especially true for local jurisdictions, given the extent to which elections are administered locally. Even where there is a substantial amount of legacy infrastructure—old systems that are difficult or impossible to update—much can be done to mitigate risks. These systems are described below and appropriate best practices and controls are provided in Part 3.

Voter registration

Every state has a unique approach to voter registration—including some states with automatic voter registration—but there are several commonalities shared by all of them. Voter registration systems provide voters with the opportunity to establish their eligibility and right to vote, and for states and local jurisdictions to maintain each voter's record, often including assigning voters to the correct polling location. Voter registration systems support pollbooks—paper and electronic—as well as provide information back to the voter as they verify their registration and look up polling locations and sample ballots.

The inputs to voter registration systems are registrations, removals due to ineligibility (e.g., an individual moving out of state, death of a voter), and record updates, most often due to an individual moving within the state. The outputs include facilitating voter lookups—such as a voter verifying they are registered, seeking a sample ballot, or finding their polling place—and transfer of voter information to pollbooks.

In all of these cases, there is a master voter database at the state level. The 2014 EAC Statutory Overview describes this database as populated in one of three broad ways:

1. A top-down system in which the data are hosted on a single, central platform of hardware and maintained by the state with data and information supplied by local jurisdictions,
2. A bottom-up system in which the data are hosted on local hardware and periodically compiled to form a statewide voter registration list, or
3. A hybrid approach, which is a combination of a top-down and bottom-up system.

For all three cases, voter registration systems consist of one or more applications that leverage general-purpose computing systems built on commercial-off-the-shelf (COTS) hardware and software. Because they use these common computing platforms, voter registration systems may be part of a shared computing system, though in many cases they are dedicated systems with dedicated software.

While jurisdictions vary in how they allow voters to apply or update their registration, in many states, the most common way voters access a registration system is through the state's department of motor vehicles (DMV).

Additionally, voters' connection to the voter registration system may run through direct means such as a county or state registration portal, or through indirect means like mailing in a registration on paper. To address this risk, many voter registration systems with which the voter would interact are separated from the "official," or production, voter registration system. Periodically, a report of changes is generated and undergoes a quality assurance review that must be certified before being entered into the production system. This can substantially reduce, for instance, an online portal as a vector of attack, though the production system may still be network connected in other ways.

In general, voter registration systems exhibit the risk characteristics of a general-purpose computing system and, more specifically, any network connected database application. To properly mitigate risks, each voter registration system within a state, and links to the voter registration system, needs a comprehensive assessment of its technical characteristics and the application of appropriate security controls.

[FIGURE 2] shows the major functions or subsystems of a voter registration system.

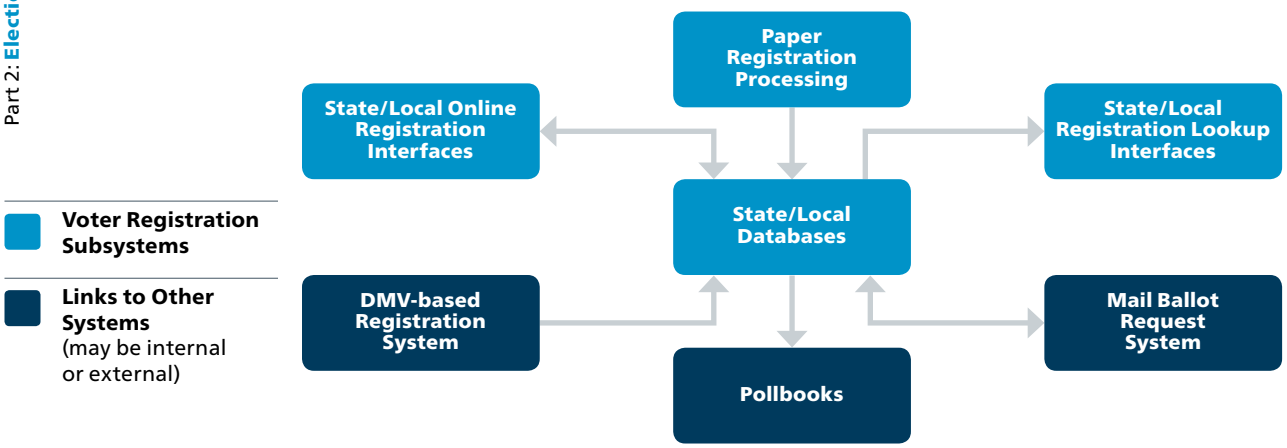


FIGURE 2: *Components of a typical voter registration system*

Types of voter registration

Voter registration generally occurs in one of two ways, each of which is recorded in a statewide registration system.

1) **Online registration:** a website or other web application allows prospective voters to register electronically and have election officials review their registration for validity, which, if valid, is entered into the voter registration database. Same-day registration, because of the need for live updating and cross checking, usually falls into this category.
2) **Paper-based registration:** prospective voters submit a paper voter registration form that is reviewed by election officials and, if valid, entered into the voter registration database. Registration of this type is out of scope in this handbook.

The type of voter registration employed at DMVs will vary by state—and perhaps locality—but should typically be viewed as a form of online registration.

Risks and threats

As noted in the previous section, the ability to access voter registration systems through the internet results in a significant increase in vulnerability and resulting risk. There are well known best practices to mitigate these risks such as those described in the box to the right, but the ability to attack and manipulate voter registration systems by remote means makes them a priority for strengthening of the security resilience of these components.

While the attacks on voter registration systems may have a specific purpose not found outside the elections domain, the vectors for those attacks, and thus the primary risks and threats associated with voter registration systems, are similar to those of other systems running on COTS IT hardware and software, and include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These items must be managed to ensure proper management of voter registration systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats. Based on their type of connectedness to digital systems, these controls are listed in Part 3.

How these components connect

Each type of voter registration, along with the master voter registration database, should have risks evaluated individually based on its type of connectivity and employ controls and best practices found in Part 3 that correspond to the type of connectivity and are appropriate to address risks. That said, aspects of the voter registration systems, and the types that may be implemented, have general characteristics that can be classified by connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

1) Online registration.

In addition, the master registration database or system itself should be considered network connected.

Indirectly Connected

N/A

In practice: protecting the voter registration database

Cybersecurity practitioners constantly face a difficult balance between convenience for users and strong security. With voter registration databases, some approaches allow elections officials to have it both ways.

Practice #1:
Officials in Washington State leverage what's called a "sneakernet" to move information from an internet-facing copy of the voter registration database and a master version of the database that is not connected to the internet. Officials have to physically move data from one machine to another—usually by moving their sneakers to walk it across the room. This doesn't eliminate all risks, but can help protect sensitive information from attack through internet-based vectors, while still allowing individuals to access their information over the internet.

Officials can only access the database from a special application. This application makes periodic copies of the database in a tightly controlled environment and these copies are used to populate all other interfaces. Similarly, changes to the master database are limited to this application. So updates from, say, the DMV don't directly access the database. They're carefully checked for corruption and moved to the master database through this controlled process.

Practice #2:
Some jurisdictions don't air gap their master voter database but use other methods to balance strong security and real-time election official access to the database. In Colorado, the master database is accessible via networks due to needs such as facilitating same-day registration. Experienced cybersecurity professionals leverage appropriate protections including strong vulnerability and risk management programs coupled with robust access controls, intrusion detection and prevention systems, web application firewalls, and security information and event management integration. Multiple layers of defenses—both computerized and human—are used to sustain operations while minimizing risk.

Not connected, out of scope

2) Paper-based registration.

Additional transmission-based risks

Transmission of a registration via email or fax leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3.

Pollbooks

Pollbooks assist election officials by providing voter registration information to workers at each polling location. Historically, these were binders that contained voter information and could be used to mark off voters when they arrived to vote. While paper pollbooks remain in use today, many pollbooks are electronic and aim to facilitate the check-in and verification process at in-person polling places. While this section focuses primarily on electronic pollbooks (e-pollbooks), it also recognizes that, depending on the implementation, producing paper pollbooks can carry transmission-based risks.

These e-pollbooks play a critical role in the voting process. They are necessary to ensure voters are registered and are appearing at the correct polling place, and their efficient use is necessary to ensure sufficient throughput to limit voters' wait times. These e-pollbooks are typically dedicated software built on COTS hardware and riding on COTS operating systems.

The primary input to e-pollbooks is the appropriate portion of the registration database. The primary output is the record of a voter having received a ballot, and in some cases providing a token to activate the vote capture device. In some cases, for instance where same-day registration is permitted, e-pollbooks may require additional inputs and outputs to allow for election day changes.

Paper pollbooks are produced from digital records, including digital registration databases. Having taken appropriate measures to mitigate risk for voter registration components, secure transmission of voter information to a printer—whether at the state or local level, or via commercial printing services—protects the integrity of the information in printed pollbooks.

Risks and threats

Attacks on e-pollbooks would generally serve to disrupt the election day process by one of these three situations: 1) attacking the integrity of the data on the pollbook by altering the information displayed from voter rolls, 2) disrupting the availability of the e-pollbooks themselves, or 3) in some cases, causing issues with the vote capture device by altering an activation token. Any of these situations could result in confusion at the polling locations and likely a loss of confidence in the integrity of election results. A successful attack of the first variety would more likely occur in voter registration systems by deleting voters from rolls or subtly modifying information in a way that prevents them from casting a ballot or forces them to use the provisional ballot process, but could also occur in the e-pollbooks themselves and during the transmission of data to the e-pollbook.

An e-pollbook may or may not be connected to a network. If they are network connected, they must be treated as having the risks of a network connected device, even if the functionality is not used. While threats are continually evolving, appropriate measures can be taken to address this largely known set of risks.

The primary cybersecurity-related risks to paper pollbooks come from the transmission of pollbook data to formatting and printing services. Data will typically be loaded onto an e-pollbook through a wired connection, a wireless network, or removable media such as a USB stick. To that end, risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities, including private networks for e-pollbooks,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, including permissions for connecting to networks and attaching removable media, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact.

These primary risks must be managed to ensure proper management of pollbooks. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Managing risks associated with e-pollbooks will generally fall into one of two classifications based on the way they can connect to load data and, if applicable, transmit data. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

Pollbook connects via a wired or wireless network.

Indirectly Connected

Pollbook connects via a physical media connection or removable media (e.g., USB sticks and other flash media that are physically connected and disconnected to other devices).

Not connected, out of scope

Paper-based pollbooks.

Additional transmission-based risks

Transmission of data for paper-based pollbooks for formatting or printing. If this transmission incorporates a digital component, it should incorporate the relevant transmission-based mitigations in Part 3.

State and local Election Management Systems

States and local jurisdictions generally have established, persistent Election Management Systems (EMSs) that handle all backend activities for which those officials are responsible. Each state has an EMS, and each local jurisdiction will typically have a separate EMS that may, but will not always, connect to the state's system. The extent to which the two systems are integrated, if at all, varies greatly.

For the most part, a local EMS is used to design or build ballots, program the election database, and report results. A state EMS typically does a wide variety of things including election night reporting and military and overseas ballot tracking.

An EMS will also typically include vote tabulation. For the purposes of this handbook, vote tabulation is broken out into its own section.

EMSs can have a wide variety of inputs and outputs that will depend on the separation of duties between the state and the local jurisdictions and the manner in which each state or local jurisdiction handles particular aspects of the election process.

Risks and threats

While EMSs are typically dedicated software that carries its own risks, that software generally runs on COTS software and hardware that operate in a networked environment. Many risks and threats associated with EMSs are similar to those of other systems running on COTS IT hardware and software, and include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in the dedicated components, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

Significant consequences may result from successful attacks on an EMS. These potential consequences include the inability to properly control election processes and systems or, depending on the functions of the EMS, incorrect assignment of ballots to their respective precincts or other errors. Furthermore, successful manipulation of an EMS could result in cascading effects on other devices that are programmed from the EMS, potentially including voting machines and vote tabulation.

How these components connect

The diversity of functions delivered by an EMS makes it difficult to generalize the level of connectedness of any given system, but most will have at least some aspects of a network connected system. A host of factors impact connectedness, such as whether a state or local EMS is network connected and whether communications with the EMS leverages connections such as a Secure File Transfer Protocol (SFTP). Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

Unless known definitively to have no network capabilities, treat an EMS as network connected.

Indirectly Connected

If known definitively to have no network capabilities, treat an EMS as indirectly connected.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Vote capture

Vote capture devices are the means by which actual votes are cast and recorded. Approaches vary greatly both across and within jurisdictions. Any given jurisdiction, and even a single polling place, is likely to have multiple methods for vote capture to accommodate both administrative decisions and different needs of voters.

For instance, on election day, a polling place may give voters the choice of electronic machines or paper ballots. Another instance, voters with language needs or voters with disabilities may necessitate the use of additional components or a separate device.

To this end, providing specific recommendations around vote capture security is a detailed task. The EAC, in coordination with other federal partners, state and local governments, vendors, and others in the elections community, maintain standards and a certification program for vote capture devices. We will not try to replicate or alter those recommendations here, but we will provide a generalized set of recommendations that can help guide officials toward best practices for vote capture devices.

Vote capture devices are often top of mind when thinking of election security—and for good reason. Vote capture devices are where democracy happens: the voices of the people are heard via the ballots they cast. But, as documented throughout this handbook, they are a single part of a larger ecosystem for which a holistic security approach is necessary. Much attention has been paid to vote capture devices, and these efforts should continue; ensuring the security of vote capture devices, like any aspect of security, is a continuous process.

Principles and more through the VVSG

The EAC is currently in the process of developing the Voluntary Voting System Guidelines (VVSG) version 2.0. The draft recommended by NIST and the EAC's Technical Guidelines Development Committee incorporates many of the best practices described within this handbook, such as auditability, access controls, data protection, system integrity, and detection and monitoring. The recommended draft is written as a high-level set of principles and guidelines, allowing specific requirements to change without requiring the full EAC approval process. This provides nimbleness and flexibility in voting systems and their underlying cybersecurity as requirements can be developed and mitigations implemented as threats are identified. More information about the VVSG 2.0 development and proposed draft can be found on the EAC's website.

The primary inputs to vote capture devices are the ballot definition file—which describes to the device how to display the ballot—as well as an activation key (for some electronic machines) and the ballot itself for scanning of a paper ballot. The primary output is, of course, the cast vote record.

In cybersecurity, we often talk about non-repudiation: the inability to deny having taken an action. Our democracy is founded in the opposite principle: your ballot is secret; no one should be able to prove who or what you voted for—or against—in the voting booth. This presents an inherent difficulty in maintaining the security of the voting process. We intentionally create voter anonymity through a breakpoint between the fact that an individual voted and what votes they actually cast. We never want to enable the ability to look at a marked ballot and track it back to a specific voter.

Instead, we must carefully protect the integrity and secrecy of the vote cast through the capture process and into the process of tabulation. To do this, best practices call for applying a series of controls to mitigate the risk that a vote capture device is functioning improperly, to identify problems if they occur, and to recover without any loss of integrity.

Types of vote capture processes

Vote capture generally occurs in one of six ways:

1) **Voter marked and hand counted paper balloting.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, collected, and counted by hand. Hand counting represents a relatively small share of total votes. This category usually covers some mail-in ballots.
2) **Voter marked paper balloting with scanning.** Ballots are typically pre-printed or printed on demand, given to voters who fill them out by hand, and collected. Votes are tabulated by scanning the paper ballot with an optical or digital scanner, either individually or in batches. This category covers some mail-in ballots.
3) **Electronic marking with paper ballot output.** Rather than handing out a paper ballot, the voter is directed to a machine that displays the ballot. The voter casts votes, and the machine prints a marked ballot. These printed ballots are tabulated either individually or in batches. Votes are usually tabulated by scanning the paper ballot with an optical or digital scanner, though are sometimes counted by hand. The vote capture device does not store a record of the vote selections. This type of vote capture device is commonly referred to as a *ballot marking device.*
4) **Electronic voting with paper record.** The voter is directed to a machine that displays the ballot. The vote is captured on the machine and either transmitted digitally to a central machine for tabulation, or removable media is extracted from the machine at a later time to transmit a batch of captured votes. At the time the vote is captured, the machine creates a printed record of the vote selections that the voter can verify. That record remains with the machine. This type of vote capture device is commonly referred to as a *direct record electronic (DRE) device with voter verifiable paper audit trail.*
5) **Electronic voting with no paper record.** The same as electronic voting with paper record, but the machine does not print a record of the captured vote. Captured votes are only maintained digitally, typically in multiple physical locations on the device and, sometimes, on a centrally managed device at the polling location. This type of vote capture device is commonly referred to as a *DRE device.*
6) **Electronic receipt and delivery of ballots conducted remotely.** The majority of ballots received by voters using this method are voters covered by the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). Though most UOCAVA votes involve paper ballots, there is a sub-set of this population that submits their marked ballot in a digitally-connected method such as email or fax. Once received digitally, the voter's vote selections are transcribed so that the vote selections are integrated into the vote tabulation and results reporting systems; these systems do not have network connections to the voting system. When this approach is used, the balloting itself is out of scope as it is via paper means. However, this type of voting can carry transmission-based risks.

Risks and threats

The consequences of a successful attack in a vote capture device are significant: the intentions of a voter are not properly reflected in the election results. The vast majority of vote capture devices are not network connected systems. This helps limit the attack paths and therefore the risks to which they are subject—in cybersecurity parlance, a non-networked approach substantially reduces the attack surface. Therefore, to change a large number of votes typically requires access to the vote capture machine hardware or software, or the ability to introduce errors through the devices that program the vote capture device or download results from the vote capture device. Moreover, most vote capture devices are tested and certified against criteria defined by the EAC, a state or local entity, or both, though evolving threats can change the risk profile of a device even if it has previously been certified.

The type of vote capture device we call *electronic receipt and delivery of ballots conducted remotely* can take on a large number of flavors. In terms of cybersecurity-related risks, for activities like emailing ballots, election officials must consider especially risks involved in the transmission of the ballot. Whether during distribution or return, if the transmission of the ballot is done via digital means, it is subject to the risks of that transmission mode. In Part 3, there is a set of control measures that provide mitigations for risks in transmission.

Regardless of approach, risks exist, and they mostly stem from the transfer of data to or from vote capture machines. Specifically, they include:

- If ever networked, risks associated with established (whether persistent or intermittent) network connectivity,
- Risks associated with the corruption of removable media or temporary physical connections to systems that are networked,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users, and
- Difficulty associated with finding, and rolling back, improper changes found after the fact, especially in the context of ballot secrecy.

How these components connect

Each type of vote capture process should have risks evaluated individually based on its type of connectivity. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Although many jurisdictions program the vote capture devices with the ballot definition using indirectly connected methods, some use methods to load the ballot definition files to the vote capture device by transmitting the data over a closed-local area network.

Also, many central count scanners, used for *Voter marked paper balloting with scanning* in batches (usually vote by mail ballots) are similarly networked on a closed-LAN.

Some electronic vote capture machines also directly transmit data for election night reporting.

Indirectly Connected

2) *Voter marked paper balloting with scanning.* Paper ballots do not include an electronic component. While scanners are not typically network connected devices, they must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.
3) *Electronic voting with paper ballot output.* In addition to the role of the scanners, the vote capture machines are typically not network connected, but must be programmed to display the ballot and print the ballot in the correct format.
4) *Electronic voting with paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.
5) *Electronic voting with no paper record.* The vote capture machines are typically not network connected but must be programmed to understand the ballot format and must transmit captured vote data to another, usually network connected, device.

NOTE: If a vote capture machine transmits data for any reason—or even if the functionality is enabled regardless of whether it is used—it should be considered *network connected.*

Not connected, out of scope

1) *Voter marked and hand counted paper balloting.* Out of scope in this handbook as the vote capture process does not include a digital component.

Additional transmission-based risks

6) *Electronic voting conducted remotely.* These methods vary greatly and must be addressed on a case-by-case basis. At minimum, when web-based, email, or fax transmission is used in either direction, it leverages a digital component and should incorporate the relevant transmission-based mitigations in Part 3. Aspects definitively executed without a digital component are *not connected, out of scope.*

Vote tabulation

In its broadest definition, vote tabulation is any aggregation or summation of votes. Vote tabulation is the aggregation of votes (e.g., cast vote records and vote summaries) for the purpose of generating totals and results report files. For the purposes of this handbook, this section on vote tabulation is considered separately from both the EMS of which tabulation is usually a part, and vote capture machines that also tabulate (or aggregate). Vote tabulation in this handbook is focused on tabulation occurring across precincts, counties, etc., and covers both official and unofficial vote tabulation.

Risks and threats

Similar to vote capture devices, attacks on vote tabulation would seek to alter the counting of cast votes. This impact would be felt through the determination of the election outcome as well as the potential for confusion if initially reported outcomes did not agree with later certified results.

Vote tabulation typically involves either dedicated software or COTS software running on COTS hardware and operating systems, though some dedicated hardware is also in use. Vote capture devices most often transmit the vote data (e.g., results, cast vote records) to the vote tabulation system using removable media, though sometimes that data is transmitted across a network. Vote data is most often transferred across jurisdictions and to the state through uploads via direct connections such as a virtual private network, local network connections, faxes, or even phone calls.

The primary risks to vote tabulation are similar to those of other COTS-based systems: a compromise of the integrity or availability of aggregated votes totals could reduce confidence in an election, if not alter the outcome. Though the vote data is likely loaded to these systems via removable media, most risks stem from vulnerabilities in these networked systems themselves. Such risks and threats include:

- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Lack of confidentiality and integrity protection for transmitted results,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

These primary risks must be managed to ensure proper management of vote tabulation systems. Because they are risks and threats shared among users of COTS products, there is a well-established set of controls to mitigate risk and thwart threats.

How these components connect

Depending on the implementation, these systems should be considered network connected or indirectly connected. They may interface with the internet, and, even if they do not, almost certainly interface with a system that is connected to a network. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, vote tabulation equipment will be *network connected,* whether through a wired or wireless connection.

Indirectly Connected

If vote tabulation equipment is no*t network connected,* it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Election results reporting and publishing

After votes are tabulated, results must be communicated both internally and to the public. In any given state, this can take many forms, but, in most cases, the basic process goal remains: getting results as quickly and accurately as possible. This section focuses on election night reporting, which involves unofficial results.

The inputs to election results reporting and publishing tabulated votes as described in the previous section. The systems used for reporting and publishing are likely networked, and, in many cases, have public facing websites.

The outputs are the unofficial election results, typically published on a website, often in multiple formats such as extensible markup language (XML), hypertext markup language (HTML), portable document format (PDF), and comma-separated values (CSV). There is likely a direct and persistent network connection between the published site and the internet, though the official record of the results may be kept on a system that is not persistently connected to the internet.

Risks and threats

As noted earlier, the consequences of an attack that would impact unofficial election results reporting and publishing could be significant, resulting in loss of confidence in the correctly reported election results when they are finally posted. The primary risks to election reporting and publishing, when connected devices are used to transmit data and communicate results, are similar to those of other COTS systems. Such risks and threats include:

- Risks associated with established (whether persistent or intermittent) internet connectivity,
- Network connections with other internal systems, some of which may be owned or operated by other organizations or authorities,
- Security weaknesses in the underlying COTS products, whether hardware or software,
- Security weaknesses in proprietary products, whether hardware or software,
- Errors in properly managing authentication and access control for authorized users,
- Difficulty associated with finding, and rolling back, improper changes found after the fact, and
- Infrastructure- and process-related issues associated with backup and auditing.

How these components connect

Depending on the approach to submitting tabulated votes, the reporting component may be network connected. The publishing component is almost certainly network connected, but may be indirectly connected, depending on the implementation. Based on the type of connectivity for a given implementation, Part 3 provides mitigations for these risks.

Network Connected

In some cases, election night reporting will be n*etwork connected,* whether through a wired or wireless connection.

The publishing component of election night reporting is almost certainly *network connected,* whether through a wired or wireless connection.

Indirectly Connected

If the election night reporting process is not network connected, it is indirectly connected through removable media.

Not connected, out of scope

N/A

Additional transmission-based risks

N/A

Part 3: **Mitigating System Risk**

Critical activities and best practices in elections infrastructure security.

Mitigating risk is, ultimately, about decisions and actions that establish trust in aspects of a system, leading to confidence in the outcome. Risk must be considered at every stage of a system – requirements, design, development, operation, and even for disposal or retirement (e.g., removal of sensitive information).

Like many systems, for election systems this involves establishing trust in users, devices, software, and processes. Many systems are "composed," or built up from a variety of commercial and purpose-built parts, devices, and software connected via processes and user actions. The results in security decisions about trust are made across many components and brought together at a system level. In other cases, key election system components or services functions are contracted out. This does not change the security responsibility for decision-makers, but forces them to think about how the desired security properties can be specified in contract language and service specifications, rather than implemented directly.

This part of the handbook contains:

1. A set of critical risk-mitigating activities from which all organizations can benefit,
2. Recommendations for best practices in contracting for IT services, and
3. A set of best practices in the form of recommendations and controls for network connected and indirectly connected devices, as well as for transmission of information.

Critical risk-mitigating activities

Auditing

Election officials conduct many audits of all aspects of the election process (e.g., vote by mail processing, training, equipment delivery) and election systems (e.g., voter registration transactions, audit log data). However, the focus of this section is on auditing vote capture and tabulation in an election.

Objective auditing in Linn County

In Iowa, Linn County Election Services hired a cybersecurity firm to conduct an audit of various aspects of the county's elections infrastructure. The firm submitted recommendations, and the county decided which of those to prioritize for implementation. The goal in hiring a third-party vendor was to provide objective, professional advice and assistance. This helps ongoing security efforts and gives confidence to the public that Linn County is taking cybersecurity seriously in its elections.

Included in this is to validate that the aggregated results reflect the actual ballots cast. One auditing approach is to select a sample of the ballots and, applying a structured process, do a partial recount of the ballots. This controlled audit is intended to provide confidence that the voting results are accurate based on the results of that partial recount. Moreover, audits provide information to election officials that go beyond the requirements for audit and recounting results; audits are the "production time" opportunity for election officials to know that the systems they are using are working properly.

The approach to auditing can vary based on a number of factors, including requirements that may be established within elections jurisdictions. Some auditing requirements call for a manual recount of a set percentage of ballots, others—including risk limiting audits described below—leverage statistical methods to determine the extent of the recount. Auditing requirements typically also have a trigger for a larger recount or full recount based on the outcome of the initial audit. Given the potential expense of auditing, it is critical to properly design audit procedures to reduce costs while achieving the goals of the audit.

Almost all states have provisions for a full recount of a contest should the result of that contest fall within the state required recount margin (for instance, many states require a recount for a statewide race if that race is within one half of one percent after certification).

The initial audit size and recount triggers are critically important to a good audit. As important is the method by which the audited ballots are selected. Establishing proper methods for random selection of ballots can have a tremendous impact on the audit's ability to confirm election results or show evidence of tampering.

For election officials, the first step to a good audit is recognizing that records must be kept in order to make an audit possible. This means allocating resources to support an audit, along with procedures for efficiently executing the audit and making it sufficiently transparent for interested parties. While audits are not inherently digitally-based efforts, establishing an audit process, with resources, ballot selection methods, audit size rules, and recount triggers, is a critical aspect of mitigating risk across all aspects of elections.

A best practice: risk limiting audits

A possible weakness in some traditional auditing methods is that often either more ballots or fewer ballots are recounted than necessary to validate the results. This can either produce an audit that doesn't fully validate the outcome of the election, or an audit that is more costly than necessary without increasing confidence in the results.

More recently, the concept of risk limiting audits has been introduced as an approach to auditing election results that is both effective and efficient. In addition to those characteristics necessary in a traditional audit—resources, good ballot selection methods, and prior-determined rules—in a risk limiting audit the size of the audit and recount triggers are based on a "stopping rule" determined by the likelihood that the actual election outcome differs from the reported outcome. Put another way, additional ballots are recounted in the audit until there is a pre-determined statistical level of confidence that the reported result is correct. As an example, a very large margin of victory will typically result in a relatively small audit size, as a very large error would have to occur to change the outcome. A very close election, on the other hand, would require a larger audit.

In a risk limiting audit, the size of the audit is determined by the results of the audit itself. That is, the closer the audited results are to the actual outcome, the sooner the audit ends. This is termed the statistical confidence in an election's results. As soon as a previously-determined confidence threshold is met, the audit can stop. As in all audits, units—precincts, machines, batches of paper records—should be selected using random sampling methods. In a risk-limiting audit, the sample size will depend on the margin of victory and other factors; these other factors may include the number of ballots in each precinct and the overall number of ballots in the contests. In general, smaller margins of victory and fewer total votes cast require auditing a larger percentage of the ballots cast. These methods are well-documented and replicable through sources such as ElectionAudits.org.

In practice: risk limiting audits in Colorado

Recently, the state of Colorado established a legal requirement that all elections be subjected to a risk limiting audit. The Colorado Secretary of State defines the "risk limits" for each election. The risk limits (i.e., the acceptable probability that the election results might not be correct based on the statistical analysis process implemented within the risk limiting audit) will guide the process of selecting the size and distribution of the sample to be subjected to the initial audit, and in turn successive audits if they are required to achieve the risk limit confidence. The trend of leveraging risk limiting audits continues to gain steam, and election organizations should consider Colorado as a use case from which they can learn. The References section of this handbook provides additional information on Colorado's approach.

Incident response planning

Despite the best efforts of election officials and their technical staff, there is some likelihood that there will be an incident at some point during an election cycle. This is the nature of cybersecurity; the true measure of success is often the resiliency of an organization in the face of these incidents.

Incidents can be minor, having no real potential for impacting the election results or public perception of the elections process, or they could be major incidents requiring prompt action to ensure the actual or perceived integrity of the election results. An incident could be a direct attack on some portion of the election system, or it could be a potential threat that might affect confidence in the system (e.g., a reported major flaw in a foundational COTS component of many election systems).

Experience shows that successful incident response depends almost entirely on planning and preparation—the work done before any incident occurs. Good technical and process controls will minimize the attack surface and also help to enable timely analysis of the incident. Identifying key decision-makers and their roles ahead of time allows for effective response.

Planning and preparing begins with creating a plan for diagnosing and recovering from incidents and exercising this plan. To properly develop and exercise these plans, efforts must include a wide variety of stakeholders—ideally all stakeholders that would be involved in response to and recovery from the incident itself. All stakeholders, including seemingly sovereign ones such as federal, state, and local officials, must collaborate in incident response and recovery; they must also collaborate in preparing for those incidents. As the threats change, so must plans. Officials must update documentation regularly and include specific plans for addressing modern cybersecurity risks, such as those presented throughout Part 2.

When an incident occurs, time is often the most important factor in minimizing impact. To this end, each individual involved in the response should immediately know what to do. Exercising plans can facilitate this, and best practice calls for conducting one or more formal incident exercises that would assess preparation and response for a set of potential incident scenarios.

Exercises should occur regularly, including during each election cycle. These exercises present an opportunity to understand roles and responsibilities, test and refine a communications strategy, and identify needs for external support such as from outside technical, legal, or communications experts. These exercises help the elections team and leadership understand that the initial assessment of the incident is often not the final assessment and that deliberate actions must be taken to ensure an appropriate response.

A large part of these exercises is about coordination with peers and partners. Regardless of how an organization prepares for an incident, whether in elections or anywhere else, maintaining good relationships and open communication has an impact when trouble arises. Individuals in all capacities of the elections process need to know where to get information, who to call both within and external to their organization, and how to continually educate themselves on how the environment is changing.

Incident recovery

Like incident response, having plans and processes in place before an incident greatly increases the likelihood of swift recovery with minimum downtime and losses. The incident response measures above will dictate the response to an incident, but not always the actions necessary to recover from the incident.

In practice: recovery ready in Cook County and California

In Illinois, since 2007, the Cook County Clerk's office has worked with an independent data analysis firm, Data Defenders, LLC, which has implemented its Applied Computer Forensics process, called Election System Auditing (ESA)™, as part of an overall election integrity management plan.

For each election, the forensics process takes three "snapshots" of the election equipment: one prior to pre-election logic and accuracy testing (Pre-LAT), one immediately after Pre-LAT, and a final one after the election has finished and the equipment is returned from the polling places and early voting sites.

These snapshots capture all of the information that makes up the software and firmware. Snapshots are encrypted and hashed so that any tampering with the snapshot will be immediately detectable. The three snapshots' hash values are compared with each to see if the software has been altered at any stage of the election process.

A reference copy of all software and firmware used by the voting system is obtained by the County Clerk from a third party source such as NIST or from a certified Voting Systems Testing Laboratory. The forensic analysis compares the before and after images listed above to the reference copy and reports on any discrepancies.

The reporting identifies any altered or deleted files, programs, scripts, or other operating components. In the case of a discrepancy, the analysis can recover the information and identify the precise lines of code that were added, altered or deleted.

Not all jurisdictions take this approach. In California, for example, the state requires that a master image be created and that image be reinstalled prior to every election. The master images are created using the trusted build files that are provided to the jurisdiction by the EAC or State of California. The trusted build is the file that is built from the source code that was reviewed and certified.

The decision of how often to create master images are a case-by-case decision, but the broader point remains: the ability to restore from a backup is critical to graceful recovery, and the ability to compare a system to a known good state is critical for identifying problems.

Incident response generally follows a lifecycle of: prepare; detect and analyze; contain, eradicate, and recover; and manage post-incident. Again, it begins with documenting and exercising, but in recovery this includes specific information about the systems and processes that may be impacted, such as knowing the hardware and software comprising specific systems, as well as things such as hashes of critical files—a way to validate whether a file has been tampered with from its last known good state. In preparing for incident recovery, one of the most critical mitigation strategies is to ensure proper backups that are secured separately from the affected systems and networks in advance of a potential incident.

The process of actually recovering starts with understanding the incident. As part of that analysis, decision-makers need to understand the impact of the incident so they can prioritize resources appropriately. Recovery is about getting back to a viable state—in some cases, the priority isn't to directly fix the problem, but rather to work around it to get to the desired outcome without the affected system. This is nothing new in the elections context: when a vote capture device breaks, it may be desirable to fix it, but it may be better at the moment to move to paper ballots so votes can be cast efficiently. The same logic may apply in a cybersecurity context across the elections ecosystem; the most important reaction is often to return to an operational state, even if it's not the optimal state.

Recovery, then, is about getting to the best possible outcome in light of the current circumstances. With proper planning and exercising, officials can avoid the impact of an incident that could prevent successfully executing an election, even when seemingly all has gone wrong.

Attacks such as those that would be directed at an election come with a motivation to impact the election in some way. Nothing serves as a greater disincentive to an attacker than knowing that their target will recover quickly and completely. And little serves to build trust with the public like a plan to achieve an accurate result even if an attack is successful. Just as with other aspects of cybersecurity, by taking the time to prepare before an incident occurs, election officials can actually turn away attackers before they arrive.

Contracting for systems or services

Many organizations use contractors or vendors to provide election system components and services to support elections processes or elections system operations. Election officials should assess the contracted supply chain in addition to support provided internally. In instances where there is contract support, officials should carefully analyze requirements for security and clearly define them in the contract. The government organization that is doing the contracting has the responsibility to assess the security risks for the component or service based on an evaluation of potential threats and security weaknesses or vulnerabilities as well as the probability of occurrence and resulting consequences. Security considerations should be an important consideration in the process of evaluating and selecting a contractor.

If the elections staff is contracting for services that are managed by a contractor or vendor, such as hosting of elections-related software or operations of elections systems, the contract should require that the company providing managed services also provide documentation of their cybersecurity processes and controls, including security metrics that are being collected and monitored. Contractor controls can then be compared to the controls listed in this handbook.

The contract should include a definition of services to be delivered (called a service level agreement or SLA) that includes security controls identified in this handbook. Moreover, a best practice would be that the contractor is subjected to regular independent audits of security controls, with results available to the government organization. Elections officials may wish to have their own security audits. The contract will need to provide for this and the elections officials will need to set aside funds for the audits.

For elections system components that are subject to elections system certification requirements, evidence of certification is required. Ideally, there should also be a provision for the contractor to provide security updates to the component over its lifecycle to ensure that vulnerabilities that are discovered are corrected and the component is recertified. For system components or services that are not subject to certification, security requirements will need to align with the particular capabilities or services provided in the contract. Many of the best practices listed in this handbook may be appropriate to include as contract requirements.

In general, the contract should require that the contractor provide a security plan as one of the initial contract deliverables. The security plan should describe how the contractor will meet the security obligations of the contract and specify the security practices and procedures that will be used. Of particular importance in specifying security requirements for contractors will be to address how elections-sensitive information (e.g., ballot layout, voter personal information, vote results) is protected during the execution of the contract and how information records are destroyed.

Additionally, contracts should address the obligations of contracted system operators and public sector clients in regards to identity theft liability, control of and access to public and private data under open records laws, and incident response plans and processes. Where possible, contracts also should specify that vendors transmit network, system, and application logs to the client's security information and event management tools if the client requests. This would allow election officials and their staffs to review and monitor activity instead of being solely reliant on the vendor's capacity for monitoring.

Guidelines for ensuring security of contracted support has been described in the publication ISO/IEC 27002. Specifically, section 15 of the standard describes security issues that should be addressed in dealing with suppliers. The Appendix to this handbook contains a reproduction of this section. Contracting and technical personnel are encouraged to use this or a similar resource to help identify and assess potential risks as well as responsibilities that will need to be addressed in contract documents and in managing suppliers.

Security best practices

These recommendations are derived from extensive experience understanding the types of vulnerabilities found and attacks experienced across a very wide variety of enterprises, and then translating that into specific and positive steps to mitigate those vulnerabilities and threats. Those recommendations are tailored based on the system and "mission" issues that are unique to elections systems, and the confidence expected for successful outcomes. The process used also examined the various guidelines and specifications used in this sector in order to maintain consistency and minimize overlap.

All of the recommended practices are grouped by class of connectedness (i.e., network connected, indirectly connected, transmission), which was identified as the key factor in assessing security risk. In addition, recommended practices that specifically deal with transmission (electronically or manually) are grouped as a collection for ease of reference.

Network Connected

Network connected components work directly with other devices or systems to achieve their objectives. These connections provide many benefits (e.g., remote diagnostics and management, simple data transfer, rapid updating), but also introduce additional risks that must be taken into consideration when managing the lifecycle of the device. Most network connected devices will provide a remote means to accessing and managing the devices, which means organizations must take extra efforts to protect access to those capabilities. Network connected devices do not necessarily have to be connected to the internet.

Indirectly Connected

Indirectly connected components are not persistently interconnected with other devices. They do, however, have to exchange information in order to complete their objectives in the election process. While these devices do not carry the same risks associated with being connected to a network or the internet, connecting these components to other devices, either through the use of removable media or direct wired connects, can introduce threats. Mitigating these risks requires a particular set of controls and recommendations when managing the device.

Transmission

In addition to the level of network connectedness, recommendations to address the broader risk of transmission of information across systems are listed separately. These can provide different and sometimes unexpected avenues of attack. These can also involve information transmitted to or from supporting systems that are easy to overlook in terms of security criticality (e.g., the printing of pollbooks, scheduling systems).

Structure of the best practices

Each best practice includes the following information:

- Asset Class (Device, Process, Software, User) — the portion of the overall system to which the practice applies.
- Priority (High, Medium, Low) — from a security perspective (in this handbook, only High and Medium practices have been included).
- Applicable CIS Controls — a cross-reference to the most applicable of the CIS Controls (which can provide a deeper description of this type of practice, and pointers to other information).

We also provide information intended to help decision-makers calibrate the potential challenges of implementation. However, these should be treated as rough guidelines for a "typical" situation – not a rule that can be applied to every election system.

- Potential User Resistance (Yes/No) — Would implementation of the practice be expected to cause resistance or complaints by users and operators of the system? If so, extra care might be needed for rollout or training; and care should be taken so that implementation doesn't encourage the use of risky "work-arounds."
- Upfront Cost (High, Medium, Low) — Does this practice typically require the purchase of new technology, or other significant capital expenditure (High)? Items can be listed as Low when no separate purchase is needed, often because the recommendation can be implemented using existing technology, into the basic configuration of the purchased system, or through operator action.
- Operational Cost (High, Medium, Low) — What are the expected post-purchase costs of this practice? Are there high costs associated with things like supplies (e.g., media, special licensing)?

Summary of connectedness in elections infrastructure components

Part 2 describes the components of a generalized elections system. The end of each subsection classified the different approaches to implementing each component based on the extent to which the component is connected to networks. These connectedness classifications are summarized in Table 1 and form the basis of the best practices. Depending on specific implementation, some of these classifications may vary. However, unless compelling information suggests otherwise, components should be protected at the level indicated.

From Part 2, election officials and others should be able to step through each component to determine the manner (or manners) in which it is implemented in a given election jurisdiction. Once the approach is known, the connectedness classification, summarized here, maps to specific sets of best practices found in the remainder of Part 3.

As noted in Part 2, the components below are a subset that, in our view, reflect the highest risk targets. For digital components not listed below, the analysis methods described in Part 2 can be applied to determine the appropriate correctness class and the associated best practices applicable to that component.

Practitioners can implement these best practices in any order, but we recommend beginning with the high priority best practices.

TABLE 1:

Summary of connectedness for elections infrastructure components

Component		Type within component	Connectedness Class
Voter registration		Master systems and databases	Network connected
	1	Online	Network connected
	2	Paper-based	Not connected
		Transmission of a registration via email or fax	Transmission-based
Pollbooks		e-Pollbook, connects via a wired or wireless network	Network connected
		e-Pollbook, connects via a physical media connection or removable media	Indirectly connected
		Transmission of data for printing via a network connection, website portal, or email	Transmission-based
		Transmission of data for printing via a wired media connection or removable media	Transmission-based
EMS	1	Unless definitively known to have no network capabilities	Network connected
	2	If known definitively to have no network capabilities	Indirectly connected
Vote capture		Vote capture device transmits data for any reason—or if the functionality is enabled regardless of whether it is used	Network connected
	1	Voter marked and hand counted paper balloting	Not connected
	2	Voter marked paper balloting with scanning	Indirectly connected
	3	Electronic voting with paper ballot output	Indirectly connected
	4	Electronic voting with paper record	Indirectly connected
	5	Electronic voting with no paper record	Indirectly connected
	6	Electronic receipt and delivery of ballots conducted remotely	Transmission-based
Vote tabulation	1	Connects via a wired or wireless connection	Network connected
	2	All others	Indirectly connected
Election night reporting	1	If receiving tabulated votes via a wired or wireless connection	Network connected
	2	If receiving tabulated votes via a wired media connection or removable media	Indirectly connected
Election night publishing	1	All	Network connected

Best Practices

The following best practices address the risks identified elsewhere in this handbook. References to resources are listed in the Appendix.

Connectedness Class
Network Connected

Priority
High

1 Whitelist which IPs can access the device

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

2 Regularly scan the network to ensure only authorized devices are connected

Applicable CIS Controls

#1.1: Automated Asset Inventory Tool
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

#12.8: Periodically Scan For Back-channel Connections To The Internet
Periodically scan for back-channel connections to the Internet that bypass the DMZ, including unauthorized VPN connections and dual-homed hosts connected to the enterprise network and to other networks via wireless, dial-up modems, or other mechanisms.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
Automated tools should be available to actively scan the internal environment, while DHS and MS-ISAC services can assist organizations with scanning their externally facing assets.

3 Limit the devices that are on the same subnet to only those devices required

Applicable CIS Controls

#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
NIST guidance is available to help the technical team determine how to appropriately segregate assets and permit access to only those devices or systems requiring access: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

continued:

Connectedness Class	Priority
Network Connected	**High**

4 Only utilize approved and managed USB devices with appropriate device encryption and device authentication

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know
Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization's public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources
CISCO recommendations on how to implement Access Control Lists on Perimeter Devices: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

5 Disable wireless peripheral access of devices unless required and the risk is formally approved by election officials

Applicable CIS Controls

#15.8: Disable Wireless Peripheral Access (Bluetooth, WiFi, radio, microwave, satellite, etc.) Unless Required
Disable wireless peripheral access of devices (such as Bluetooth and WiFi), unless such access is required and risk acceptance is formally documented.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Microsoft guidance on how to disable Bluetooth: https://technet.microsoft.com/en-us/library/dd252791.aspx.

6 Ensure the system is segregated from other independent election systems and non-election supporting systems

Applicable CIS Controls

#14.1: Implement Network Segmentation Based On Information Class
Segment the network based on the type of information and the sensitivity of the information processes and stored. Use virtual LANS (VLANS) to protect and isolate information and processing with different protection requirements with firewall filtering to ensure that only authorized individuals are able to communicate with systems necessary to fulfill their specific responsibilities.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	High	Medium

Resources
While this is an often overlooked control and can require architectural redesigns, this is an important control to pursue. NIST guidance on boundary protection: https://nvd.nist.gov/800-53/Rev4/control/SC-7.

7 Deploy Network Intrusion Detection System (IDS) (e.g., MS-ISAC Albert sensor) on Internet and extranet DMZ systems

Applicable CIS Controls

#12.2: Record At Least Packet Header Information On DMZ Networks
On DMZ networks, configure monitoring systems (which may be built in to the IDS sensors or deployed as a separate technology) to record at least packet header information, and preferably full packet header and payloads of the traffic destined for or passing through the network border. This traffic should be sent to a properly configured Security Information Event Management (SIEM) or log analytics system so that events can be correlated from all devices on the network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Medium

Resources
The Albert device is part of the MS-ISAC offering: https://www.cisecurity.org/ms-isac/services/albert/. There are a number of commercially-available options, such as: https://securityonion.net/.

8 If wireless is required, ensure all wireless traffic use at least Advanced Encryption Standard (AES) encryption with at least Wi-Fi Protected Access 2 (WPA2)

Applicable CIS Controls

#15.5: Protect All Wireless Traffic with AES and WPA2
Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi-Fi Protected Access 2 (WPA2) protection.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Medium	Low

Resources
NIST guidance on how to implement secure wireless networks: https://www.nist.gov/publications/guidelines-securing-wireless-local-area-networks-wlans.

9 Use trusted certificates for any publicly-facing website

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	High	No	Low	Low

Resources
Vendor recommendation on deploying certificates with the system. Also, test to verify SSL certificate configuration, with products such as with Qualys: https://www.ssllabs.com/ssltest/.

10 Ensure logs are securely archived

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources
Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security: https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

11 On a regular basis, review logs to identify anomalies or abnormal events

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

continued:

Connectedness Class	Priority
Network Connected	**High**

12 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls

#13.2: Deploy Hard Drive Encryption Software

Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources

Work with appropriate vendors. Additionally, see Microsoft guidance on digital signatures: https://technet.microsoft.com/en-us/library/cc962021.aspx.

13 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources

Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

14 Perform system testing prior to elections (prior to any ballot delivery), such as acceptance testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Low

Resources

Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

15 Ensure acceptance testing is done when receiving or installing new/updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Low	Low

Resources

Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

16 Conduct criminal background checks for all staff including vendors, consultants, and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	High	No	Medium	Medium

Resources

Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

17 Deploy application whitelisting

Applicable CIS Controls

 # 2.2: Deploy Application Whitelisting

Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Low

Resources

NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

18 Work with election system provider to ensure base system components (e.g., OS, database) are hardened based on established industry standards

Applicable CIS Controls

#3.1: Establish Standard Secure Configurations For OS And Software

Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

#18.7: Use Standard Database Hardening Templates

For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	High	Low

Resources

CIS Benchmarks provide hardened configurations for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/. In addition, NIST provides additional recommendations for baselines https://nvd.nist.gov/800-53/Rev4/control/CM-2. Some vendor products may require tailoring to work with benchmark configured systems. Deviations from the benchmark should be documented.

19 Regularly run a SCAP-compliant vulnerability scanner

Applicable CIS Controls

#4.1: Weekly Automated Vulnerability Scanning

Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code-based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Medium

Resources

Principal cost beyond the purchase of the tool is the adjudication and remediation of the findings. SCAP validated tools can be found at: https://nvd.nist.gov/scap/validated-tools and there are a number of other commercially available tools.

continued:

Connectedness Class	Priority
Network Connected	**High**

20 Utilize EAC certified or equivalent software and hardware products where applicable

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Medium	Medium

Resources

Guidance from EAC about their vendor certification process: https://www.eac.gov/voting-equipment/frequently-asked-questions/.

21 Store secure baseline configuration on hardened offline system and securely deploy baseline configurations

Applicable CIS Controls

#3.3: Store Master Images Securely

Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources

NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

22 Utilize write-once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	High	No	Low	Low

Resources

NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

23 Maintain detailed maintenance record of all system components

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources

Maintenance process, procedures and recommendations based on NIST guidance: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

24 Require the use of multi-factor authentication

Applicable CIS Controls

#5.6: Use Multi-factor Authentication For All Administrative Access
Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards,certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods.

#12.6: Require Two-factor Authentication For Remote Login
Require all remote login access (including VPN, dial-up, and other forms of access that allow login to internal systems) to use two-factor authentication.

#16.11: Use Multi-factor Authentication For Accounts Accessing Sensitive Data Or Systems
Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	High	Medium

Resources
Vendor specific. NIST guidance on authentication: https://pages.nist.gov/800-63-3/sp800-63b.html.

25 Require users to use strong passwords (14 character passphrases) if multi-factor authentication is not available

Applicable CIS Controls

#5.7: User Accounts Shall Use Long Passwords
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

#16.12: Use Long Passwords For All User Accounts
Where multi-factor authentication is not supported, user accounts shall be required to use long passwords on the system (longer than 14 characters).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Vendor specific. CIS Benchmarks details how this can be implemented for consumer grade operating systems and applications: https://www.cisecurity.org/cis-benchmarks/.

26 Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls

#5.1: Minimize And Sparingly Use Administrative Privileges
Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	High	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Network Connected

Priority
Medium

27 Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

28 Utilize tamper evident seals on all external ports that are not required for use and electronically deactivate ports where feasible

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

29 Maintain an inventory of assets that should be on the same subnet as the election system component

Applicable CIS Controls
#1.4: Asset Inventory Accounts For All Devices
Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over-IP telephones, multi-homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

30 Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

31 Conduct load and stress tests for any transactional related systems to ensure the ability of the system to mitigate potential DDoS type attacks

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Network Connected	Medium	No	Medium	Low

32 Limit the use of personally identifiable information. When it is required, ensure that it is properly secured and staff with access are properly trained on how to handle it.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

Resources

Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

33 Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

34 Identify and maintain information on network service providers and third-party companies contacts with a role in supporting election activities

Applicable CIS Controls

#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

35 Implement a change freeze prior to peak election periods for major elections

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Low	Low

36 Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Network Connected	Medium	No	Medium	Medium

37 Work with vendors to establish and follow hardening guidance for their applications

Applicable CIS Controls

#3.1: Establish Standard Secure Configurations For OS And Software

Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources

Vendors will typically provide recommendations on how to securely deploy and manage their systems.

continued:

Connectedness Class	Priority
Network Connected	**Medium**

38 Ensure logging is enabled on the system

Applicable CIS Controls

#6.2: Ensure Audit Log Settings Support Appropriate Log Entry Formatting
Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Medium

Resources
Work with Vendor to identify logging capabilities. CIS-CAT can check this configuration item for consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. CIS Benchmarks provides logging recommendations for major platforms: https://www.cisecurity.org/cis-benchmarks/.

39 Use automated tools to assist in log management and where possible ensure logs are sent to a remote system

Applicable CIS Controls

#6.6: Deploy A SIEM or Log Analysis Tools For Aggregation And Correlation/Analysis
Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profiles of common events from given systems so that they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	High	High

Resources
A variety of tools that have various capabilities and costs as well as the effort and rigor of the review and retention of the logs which will have varying costs. Windows Event Subscription Guide: https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

40 Where feasible, utilize anti-malware software with centralized reporting

Applicable CIS Controls

 # 8.1: Deploy Automated Endpoint Protection Tools
Employ automated tools to continuously monitor workstations, servers, and mobile devices with anti-virus, anti-spyware, personal firewalls, and host-based IPS functionality. All malware detection events should be sent to enterprise anti-malware administration tools and event log servers.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
Vendor specific.

41 Ensure only required ports are open on the system through regular port scans

Applicable CIS Controls

#9.3: Perform Regular Automated Port Scanning
Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed.

#9.1: Limit Open Ports, Protocols, and Services
Ensure that only ports, protocols, and services with validated business needs are running on each system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Checkable by CIS-CAT and other SCAP-validated tools (https://nvd.nist.gov/scap/validated-tools), and other network scanning tools such as NMAP: https://nmap.org.

42 Where feasible, implement host-based firewalls or port filtering tools

Applicable CIS Controls

#9.2: Leverage Host-based Firewalls
Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Medium

Resources
If host-based, can be verified by CIS-CAT: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on implementing firewalls: https://technet.microsoft.com/en-us/library/cc772353(v=ws.10).aspx.

43 Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Medium	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

44 Ensure vendors distribute software packages and updates using secure protocols

Applicable CIS Controls

#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Network Connected	Medium	No	Low	Low

Resources
Work with the election software vendors.

continued:

Connectedness Class	Priority
Network Connected	**Medium**

45 Maintain a chain of custody for all core devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

46 All remote connections to the system will use secure protocols (TLS, IPSEC)

Applicable CIS Controls

#3.4: Use Only Secure Channels For Remote System Administration
Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as, TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify whether secure protocols are configured consumer grade operating system: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

47 Users will use unique user IDs

Applicable CIS Controls

Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

48 Use a dedicated machine for administrative tasks to separate day to day functions from other security critical functions. (For some components this may not be practical to implement.)

Applicable CIS Controls

#5.9: Use Dedicated Administrative Machines
Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Low

Resources
For some components this may not be practical to implement.

49 Ensure that user activity is logged and monitored for abnormal activities

Applicable CIS Controls

#16.10: Profile User Account Usage And Monitor For Anomalies
Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Medium	Medium

Resources
CIS-CAT can identify these at the consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. It is desirable to have a log aggregation or SIEM system in place to aggregate and analyze logs for abnormal behaviors.

50 Regularly review all accounts and disable any account that can't be associated with a process or owner

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

51 Establish a process for revoking system access immediately upon termination of employee or contractor

Applicable CIS Controls

#16.3: Ensure System Access Is Revoked Upon Employee/Contractor Termination
Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Resources on the process potentially involved with termination process NIST: https://nvd.nist.gov/800-53/Rev4/control/PS-4.

continued:

Connectedness Class	Priority
Network Connected	**Medium**

52 Ensure that user credentials are encrypted or hashed on all platforms

Applicable CIS Controls

#16.14: Encrypt/Hash All Authentication Files And Monitor Their Access
Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
CIS-CAT can identify this configuration on consumer grade operating systems and applications, work with vendor to verify: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

53 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls

#16.5: Configure screen locks on systems to limit access to unattended workstations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Resources
Work with dedicated purpose election system vendors to verify their products. CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/.

54 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Network Connected	Medium	No	Low	Low

Connectedness Class **Priority**

Indirectly Connected High

55 For data transfers that utilize physical transmission, utilize tamper evident seals on the exterior of the packaging

Applicable CIS Controls

#13.5: Disable Write Capabilities To USB Devices

If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Medium	Low

Resources

Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

56 Disable wireless peripheral access of devices

Applicable CIS Controls

#15.8: Disable Wireless Peripheral Access (i.e. Bluetooth) Unless Required

Disable wireless peripheral access of devices (such as Bluetooth), unless such access is required for a documented business need.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	High	No	Low	Low

Resources

Windows guidance on how to restrict hardware devices: https://technet.microsoft.com/en-us/library/cc771759(v=ws.10).aspx. Best practice is the use of specially designed USB keys that allow for encryption and device authentication.

57 Ensure staff is properly trained on cybersecurity and audit procedures and audit every election in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

Resources

Work with appropriate vendors. Review EAC Guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

58 Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Medium	Medium

Resources

Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

continued:

Connectedness Class	Priority
Indirectly Connected	**High**

59 Ensure staff is properly trained for reconciliation procedures for the pollbooks to the voting systems and reconcile every polling place and voter record in accordance with local, state, and federal guidelines

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	High	No	Low	Low

60 Store secure baseline configurations on hardened offline systems and securely deploy baseline configurations

Applicable CIS Controls

#3.3: Store Master Images Securely
Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air-gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

61 Work with the vendor to deploy application whitelisting

Applicable CIS Controls

#2.2: Deploy Application Whitelisting
Deploy application whitelisting technology that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	Yes	Medium	Low

Resources
NIST guidance on how to implement application whitelisting: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf. May have to work with the vendors to implement it on their systems.

62 Utilize the most up-to-date and certified version of vendor software

Applicable CIS Controls

#4.5: Use Automated Patch Management And Software Update Tools
Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped.

#18.1: Use Only Vendor-supported Software
For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Medium

Resources
NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7.

63 Utilize write-once media for transferring critical system files and system updates. Where it is not possible to use write-once media, that media should be used one time (for a single direction off transfer to a single destination device) and securely dispose of the media.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Low	Low

Resources

NIST guidance on Media Protection: https://nvd.nist.gov/800-53/Rev4/control/MP-7.

64 Only use the devices for election related activities

Applicable CIS Controls

#5.9: Use Dedicated Administrative Machines

Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading e-mail, composing documents, or surfing the Internet.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	High	No	Medium	Low

Resources

Review EAC guidance:https://www.eac.gov/election-officials/election-management-guidelines/.

65 Maintain detailed maintenance records of all system components

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources

Maintenance process, procedures and recommendations based on NIST: https://nvd.nist.gov/800-53/Rev4/control/MA-2.

66 Limit the number of individuals with administrative access to the platform and remove default credentials

Applicable CIS Controls

#5.1: Minimize And Sparingly Use Administrative Privileges

Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	High	No	Low	Low

Resources

Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Connectedness Class
Indirectly Connected

Priority
Medium

67 Utilize tamper evident seals on all external ports that are not required for use

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

68 Ensure that all devices are documented and accounted for throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

69 Establish and follow rigorous protocol for installing tamper evident seals and verifying their integrity upon removal

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Devices	Indirectly Connected	Medium	No	Low	Low

Resources
Check to see if vendors have this information as part of their Technical Data Product (TDP). Additional information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

70 Perform system testing prior to elections (prior to any ballot delivery), such as logic and accuracy testing

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

71 Ensure acceptance testing is done when receiving or installing new or updated software or new devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

Resources
Work with appropriate vendors. Review EAC guidance: https://www.eac.gov/election-officials/election-management-guidelines/.

72 Conduct mock elections prior to major elections to help eliminate gaps in process and legal areas

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

73 Identify and maintain information on network service providers and third-party companies' contacts with a role in supporting election activities

Applicable CIS Controls

#19.5: Assemble and maintain information on third-party contact information to be used to report a security incident (e.g., maintain an email address of security@organization.com or have a web page http://organization.com/security).

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

74 Implement a change freeze prior to peak election periods for major elections

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Low	Low

75 Prior to major elections, conduct in person site audits to verify compliance to security policies and procedures

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Process	Indirectly Connected	Medium	No	Medium	Medium

76 Verify software updates and the validity of the code base through the use of hashing algorithms and digital signatures where available

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Software	Indirectly Connected	Medium	No	Medium	Low

Resources

NIST guidance on Software Integrity: https://nvd.nist.gov/800-53/Rev4/control/SI-7. For EAC certified voting systems, System Validation Tools are required which provide a process for validating the hash values on the system versus the trusted build (certified software).

77 Ensure the use of unique user IDs

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources

Individual accountability is one of the linchpins in cybersecurity and is useful for auditing events and actions taken on a system. Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

78 Ensure individuals are only given access to the devices they need for their job

Applicable CIS Controls

#14: Controlled Access Based on the Need to Know
Controlled Access Based on the Need to Know

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources

How to implement least privilege within an organization according to NIST: https://nvd.nist.gov/800-53/Rev4/control/AC-6.

continued:

Connectedness Class	Priority
Indirectly Connected	**Medium**

79 Maintain a chain of custody for all core devices

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

80 Ensure all workstations and user accounts are logged off after a period of inactivity

Applicable CIS Controls

#16.5: Configure screen locks on systems to limit access to unattended workstations

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Resources

CIS-CAT can identify this configuration on consumer grade operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Work with special purpose election system vendors to verify their products.

81 Regularly review all authorized individuals and disable any account that can't be associated with a process or owner

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Medium	Medium

Resources

Microsoft resources for managing users: https://msdn.microsoft.com/en-us/library/cc505882.aspx.

82 Ensure your organization has a documented Acceptable Use policy that users are aware of which details the appropriate uses of the system

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Users	Indirectly Connected	Medium	No	Low	Low

Connectedness Class: Transmission — Priority: High

83 Use secure protocols for all remote connections to the system (TLS, IPSEC)

Applicable CIS Controls

#3.4: Use Only Secure Channels For Remote System Administration

Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that Table5 not actively support strong encryption should only be used if they are performed over a secondary encryption channel, such as TLS or IPSEC.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Low	Low

Resources

CIS-CAT can identify whether secure protocols are configured for common operating systems and applications: https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/. Microsoft guidance on securing remote access: https://msdn.microsoft.com/en-us/library/cc875831.aspx.

84 Ensure critical data is encrypted and digitally signed

Applicable CIS Controls

#13.2: Deploy Hard Drive Encryption Software

Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data.

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	High	No	Medium	Medium

Resources

Work with appropriate vendors. Additionally, see Microsoft's How to Set Event Log Security: https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Connectedness Class: Transmission — Priority: Medium

85 Ensure the use of bi-directional authentication to establish trust between the sender and receiver

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Low

86 For data transfers that utilize physical transmission utilize tamper evident seals on the exterior of the packaging

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources

Check to see if vendors have this information as part of their product offerings. Additionally see information on tamper evident seals: http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

87 Conduct criminal background checks for all staff including vendors, consultants and contractors supporting the election process

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Medium	Medium

Resources

Examples of this include National Agency Check Criminal History: https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

88 Track all hardware assets used for transferring data throughout their lifecycle

Asset Class	Connectedness Class	Priority	Potential Resistance	Upfront Cost	Ongoing Maint. Cost
Transmission	Transmission	Medium	No	Low	Low

Resources

NIST guidance on maintaining hardware inventories: https://nvd.nist.gov/800-53/Rev4/control/CM-8.

Appendix:
References and Resources

This section provides references to the resources cited in this handbook, including Section 15 of ISO/IEC 27002, which we reproduce with permission from ISO.

In addition, the website for this handbook, https://www.cisecurity.org/elections-resources/, has additional resources, such as more best practices from local elections officials, that may be useful for readers.

CIS resources

Under the sponsorship of the U.S. Department of Homeland Security, CIS offers a number of services to U.S. State, Local, Tribal, and Territorial (SLTT) government entities at no charge. Specifically, SLTT entities can take advantage of the following resources:

- Become members of the MS-ISAC (Multi-State Information Sharing and Analysis Center) for coordination of cybersecurity readiness and response (https://www.cisecurity.org/ms-isac/)
- Access the CIS Controls—20 foundational and advanced cybersecurity actions that can eliminate the most common attacks (https://www.cisecurity.org/controls/)
- Access the CIS Benchmarks—a set of configuration guidelines to safeguard operating systems, software, and networks (https://www.cisecurity.org/cis-benchmarks/)
- Obtain membership to CIS SecureSuite—a set of integrated cybersecurity resources to help start secure and stay secure (https://www.cisecurity.org/cis-securesuite/)
- Use CIS-CAT Pro, to quickly compare and report on the configuration of systems against CIS Benchmark recommendations (https://www.cisecurity.org/cybersecurity-tools/cis-cat-pro/)
- Purchase through CIS CyberMarket—a program to improve cybersecurity through cost-effective group procurement (https://www.cisecurity.org/services/cis-cybermarket/)
- Access CIS WorkBench—a community website that serves as a hub for tech professionals to network, collaborate, discuss technical concepts, and download CIS resources (https://www.cisecurity.org/introducing-cis-workbench/)

CIS has gathered additional resources specific to the elections community at https://www.cisecurity.org/elections-resources/. In addition to an electronic version of the handbook, the site includes additional examples of best practices in use in state and local jurisdictions, as well as other resources that may be useful to organizations implementing the best practices.

CIS also provides support beyond that funded by DHS (called "partner paid" services) if needed by SLTT organizations. Examples of partner paid services include additional Albert sensors and security monitoring services as well as tailored cybersecurity support.

Individuals working for any State, Local, Tribal, or Territorial government should contact CIS at info@msisac.org to find out what's best for their organization. Commercial entities, such as vendors of election systems and service providers, are also welcomed to access many of these services, in many cases free of charge.

Other resources referenced in this handbook

Department of Homeland Security. https://www.dhs.gov/.

Designation of chief State election official, 52 USC 20509 (2014). Accessed at https://www.gpo.gov/fdsys/pkg/USCODE-2014-title52/html/USCODE-2014-title52-subtitleII-chap205-sec20509.htm.

Election Assistance Commission. https://www.eac.gov/.

Election Assistance Commission. (2015). *Election Assistance Commission Statutory Overview: 2014.* Retrieved from https://www.eac.gov/assets/1/1/2014_Statutory_Overview_Final-2015-03-09.pdf.

Financial Sector Information Sharing and Analysis Center. https://fsisac.com/.

Harris, Joseph P. (1934). *Election Administration in the United States.* Brookings Institution Press, Washington D.C. Retrieved from https://www.nist.gov/itl/election-administration-united-states-1934-joseph-p-harris-phd.

International Organization for Standardization. (2011). *Information technology—Security techniques—Information security risk management.* ISO/IEC 27005:2011. Available at https://www.iso.org/standard/56742.html.

International Organization for Standardization. (2013). *Information technology—Security techniques—Code of practice for information security controls.* ISO/IEC 27002:2013. Available at https://www.iso.org/standard/54533.html.

National Institute of Standards and Technology. (2012). *Special Publication 800-30 Rev. 1: Guide for Conducting Risk Assessments.* NIST SP800-30. Available at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final.

National Institute of Standards and Technology. (2014). *Framework for Improving Critical Infrastructure Cybersecurity.* Available at https://www.nist.gov/cyberframework.

"Principles and Best Practices for Post-Election Audits." Edited by Mark Lindeman et al., Principles and Best Practices for Post-Election Audits, 1 Sept. 2008, www.electionaudits.org/principles.html.

Volunteer Voting System Guidelines, version 1.1. (2015). *Elections Assistance Commission.* Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/.

Summary of resources referenced in this handbook's best practices

Cisco Systems, Inc. "Configuring IP Access Lists." *Cisco,* 5 June 2017, https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html.

Election Assistance Commission. "Election Management Guidelines." *U.S. Election Assistance Commission (EAC),* https://www.eac.gov/election-officials/election-management-guidelines/.

Fyodor. "Nmap." *Nmap: the Network Mapper - Free Security Scanner,* 1 Aug. 2017, https://nmap.org/.

General Services Administration. "GSA Forms Library." *Basic National Agency Check Criminal History,* 17 Aug. 2017, https://www.gsa.gov/forms-library/basic-national-agency-check-criminal-history.

Johnston, Roger G. "Tamper-Indicating Seals: Practices, Problems, and Standards." *World Customs Organization Security Meeting,* 11 Feb. 2003, http://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-03-0269.

Microsoft Corp, Inc. "Digital signatures." *Microsoft TechNet,* https://technet.microsoft.com/en-us/library/cc962021.aspx.

Microsoft Corp, Inc. "Disabling Bluetooth and Infrared Beaming." *Microsoft TechNet,* 9 Feb. 2009, https://technet.microsoft.com/en-us/library/dd252791.aspx.

Microsoft Corp, Inc. "Event Subscriptions." *Windows Server 2008 R2 and Windows Server 2008,* 22 Feb. 2013, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "How to Set Event Log Security Locally or by Using Group Policy." *How to Set Event Log Security Locally or by Using Group Policy,* 7 Jan. 2017, https://support.microsoft.com/en-us/help/323076/how-to-set-event-log-security-locally-or-by-using-group-policy.

Microsoft Corp, Inc. "Lesson 1: Managing User Accounts." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc505882.aspx.

Microsoft Corp, Inc. "Managing Windows Firewall with Advanced Security." *Windows Server 2008 R2 and Windows Server 2008,* 2 July 2012, https://technet.microsoft.com/en-us/library/cc749183(v=ws.11).aspx.

Microsoft Corp, Inc. "Securing Remote Access." *Microsoft Developer Network,* https://msdn.microsoft.com/en-us/library/cc875831.aspx.

National Institute of Standards and Technology. (2012). *Special Publication 800-153: Guidelines for Securing Wireless Local Area Networks.* NIST SP 800-153. Available at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf.

National Institute of Standards and Technology. (2013). *Special Publication 800-35 Rev. 4: Security and Privacy Controls for Federal Information Systems and Organizations.* NIST SP 800-53r4. Available at https://csrc.nist.gov/publications/detail/sp/800-53/rev-4/final.

National Institute of Standards and Technology. (2015). *Special Publication 800-167: Guide to Application Whitelisting.* NIST SP 800-167. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf.

National Institute of Standards and Technology. (2017). *Special Publication 800-63B: Digital Identity Guidelines Authentication and Lifecycle Management.* NIST SP 800-63B. Available at https://pages.nist.gov/800-63-3/sp800-63b.html.

National Institute of Standards and Technology. *National Vulnerability Database.* Available at https://nvd.nist.gov.

Onion Solutions, LLC. "Security Onion." *Security Onion,* https://securityonion.net/.

Qualys, Inc. "SSL Server Test." *SSL Server Test,* (2018), https://www.ssllabs.com/ssltest/.

ISO/IEC 27002:2013: Information technology – Security techniques – Code of practice for information security controls

15 Supplier relationships
15.1 Information security in supplier relationships
15.1.1 Information security policy for supplier relationships

Control
Information security requirements for mitigating the risks associated with supplier's access to the organization's assets should be agreed with the supplier and documented.

Implementation guidance
The organization should identify and mandate information security controls to specifically address supplier access to the organization's information in a policy. These controls should address processes and procedures to be implemented by the organization, as well as those processes and procedures that the organization should require the supplier to implement, including:

a) identifying and documenting the types of suppliers, e.g. IT services, logistics utilities, financial services, IT infrastructure components, whom the organization will allow to access its information;
b) a standardised process and lifecycle for managing supplier relationships;
c) defining the types of information access that different types of suppliers will be allowed, and monitoring and controlling the access;
d) minimum information security requirements for each type of information and type of access to serve as the basis for individual supplier agreements based on the organization's business needs and requirements and its risk profile;
e) processes and procedures for monitoring adherence to established information security requirements for each type of supplier and type of access, including third party review and product validation;
f) accuracy and completeness controls to ensure the integrity of the information or information processing provided by either party;
g) types of obligations applicable to suppliers to protect the organization's information;
h) handling incidents and contingencies associated with supplier access including responsibilities of both the organization and suppliers;
i) resilience and, if necessary, recovery and contingency arrangements to ensure the availability of the information or information processing provided by either party;
j) awareness training for the organization's personnel involved in acquisitions regarding applicable policies, processes and procedures;
k) awareness training for the organization's personnel interacting with supplier personnel regarding appropriate rules of engagement and behaviour based on the type of supplier and the level of supplier access to the organization's systems and information;
l) conditions under which information security requirements and controls will be documented in an agreement signed by both parties;
m) managing the necessary transitions of information, information processing facilities and anything else that needs to be moved, and ensuring that information security is maintained throughout the transition period.

Other information
Information can be put at risk by suppliers with inadequate information security management. Controls should be identified and applied to administer supplier access to information processing facilities. For example, if there is a special need for confidentiality of the information, non-disclosure agreements can be used. Another example is data protection risks when the supplier agreement involves transfer of, or access to, information across borders. The organization needs to be aware that the legal or contractual responsibility for protecting information remains with the organization.

15.1.2 Addressing security within supplier agreements

Control
All relevant information security requirements should be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.

Implementation guidance
Supplier agreements should be established and documented to ensure that there is no misunderstanding between the organization and the supplier regarding both parties' obligations to fulfill relevant information security requirements.

The following terms should be considered for inclusion in the agreements in order to satisfy the identified information security requirements:

a) description of the information to be provided or accessed and methods of providing or accessing the information;
b) classification of information according to the organization's classification scheme (see 8.2); if necessary also mapping between the organization's own classification scheme and the classification scheme of the supplier;
c) legal and regulatory requirements, including data protection, intellectual property rights and copyright, and a description of how it will be ensured that they are met;
d) obligation of each contractual party to implement an agreed set of controls including access control, performance review, monitoring, reporting and auditing;
e) rules of acceptable use of information, including unacceptable use if necessary;
f) either explicit list of supplier personnel authorized to access or receive the organization's information or procedures or conditions for authorization, and removal of the authorization, for access to or receipt of the organization's information by supplier personnel;
g) information security policies relevant to the specific contract;
h) incident management requirements and procedures (especially notification and collaboration during incident remediation);
i) training and awareness requirements for specific procedures and information security requirements, e.g. for incident response, authorization procedures; relevant regulations for sub-contracting, including the controls that need to be implemented;
j) relevant agreement partners, including a contact person for information security issues;
k) screening requirements, if any, for supplier's personnel including responsibilities for conducting the screening and notification procedures if screening has not been completed or if the results give cause for doubt or concern;

l) right to audit the supplier processes and controls related to the agreement;
m) defect resolution and conflict resolution processes;
n) supplier's obligation to periodically deliver an independent report on the effectiveness of controls and agreement on timely correction of relevant issues raised in the report;
o) supplier's obligations to comply with the organization's security requirements.

Other information
The agreements can vary considerably for different organizations and among the different types of suppliers. Therefore, care should be taken to include all relevant information security risks and requirements. Supplier agreements may also involve other parties (e.g. sub-suppliers).
The procedures for continuing processing in the event that the supplier becomes unable to supply its products or services need to be considered in the agreement to avoid any delay in arranging replacement products or services.

15.1.3 Information and communication technology supply chain

Control
Agreements with suppliers should include requirements to address the information security risks associated with information and communications technology services and product supply chain.

Implementation guidance
The following topics should be considered for inclusion in supplier agreements concerning supply chain security:

a) defining information security requirements to apply to information and communication technology product or service acquisition in addition to the general information security requirements for supplier relationships;
b) for information and communication technology services, requiring that suppliers propagate the organization's security requirements throughout the supply chain if suppliers subcontract for parts of information and communication technology service provided to the organization;
c) for information and communication technology products, requiring that suppliers propagate appropriate security practices throughout the supply chain
d) if these products include components purchased from other suppliers;
e) implementing a monitoring process and acceptable methods for validating that delivered information and communication technology products and services are adhering to stated security requirements;
f) implementing a process for identifying product or service components that are critical for maintaining functionality and therefore require increased attention and scrutiny when built outside
g) of the organization especially if the top tier supplier outsources aspects of product or service components to other suppliers;
h) obtaining assurance that critical components and their origin can be traced throughout the supply chain; obtaining assurance that the delivered information and communication technology products are functioning as expected without any unexpected or unwanted features;
i) defining rules for sharing of information regarding the supply chain and any potential issues and compromises among the organization and suppliers;

j) implementing specific processes for managing information and communication technology component lifecycle and availability and associated security risks. This includes managing the risks of components no longer being available due to suppliers no longer being in business or suppliers no longer providing these components due to technology advancements.

Other information
The specific information and communication technology supply chain risk management practices are built on top of general information security, quality, project management and system engineering practices but do not replace them.

Organizations are advised to work with suppliers to understand the information and communication technology supply chain and any matters that have an important impact on the products and services being provided. Organizations can influence information and communication technology supply chain information security practices by making clear in agreements with their suppliers the matters that should be addressed by other suppliers in the information and communication technology supply chain.

Information and communication technology supply chain as addressed here includes cloud computing services.

15.2 Supplier service delivery management

15.2.1 Monitoring and review of supplier services

Control
Organizations should regularly monitor, review and audit supplier service delivery.

Implementation guidance
Monitoring and review of supplier services should ensure that the information security terms and conditions of the agreements are being adhered to and that information security incidents and problems are managed properly.

This should involve a service management relationship process between the organization and the supplier to:

a) monitor service performance levels to verify adherence to the agreements;
b) review service reports produced by the supplier and arrange regular progress meetings as required by the agreements;
c) conduct audits of suppliers, in conjunction with review of independent auditor's reports, if available, and follow-up on issues identified;
d) provide information about information security incidents and review this information as required by the agreements and any supporting guidelines and procedures;
e) review supplier audit trails and records of information security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
f) resolve and manage any identified problems;
g) review information security aspects of the supplier's relationships with its own suppliers;
h) ensure that the supplier maintains sufficient service capability together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster (see Clause 17).

The responsibility for managing supplier relationships should be assigned to a designated individual or service management team. In addition, the organization should ensure that suppliers assign responsibilities for reviewing compliance and enforcing the requirements of the agreements. Sufficient technical skills and resources should be made available to monitor that the requirements of the agreement, in particular the information security requirements, are being met. Appropriate action should be taken when deficiencies in the service delivery are observed.

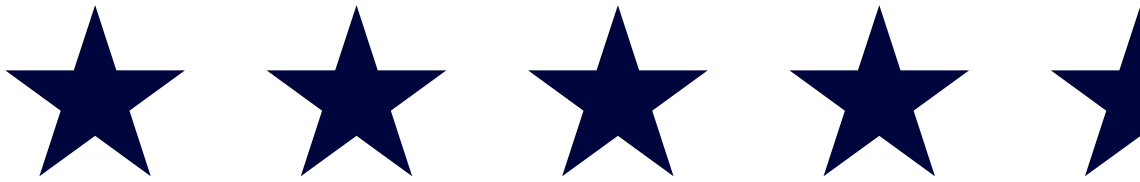
The organization should retain sufficient overall control and visibility into all security aspects for sensitive or critical information or information processing facilities accessed, processed or managed by a supplier. The organization should retain visibility into security activities such as change management, identification of vulnerabilities and information security incident reporting and response through a defined reporting process.

15.2.2 Managing changes to supplier services

Control
Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business information, systems and processes involved and reassessment of risks.

Implementation guidance
The following aspects should be taken into consideration:

a) changes to supplier agreements;
b) changes made by the organization to implement:
    1) enhancements to the current services offered;
    2) development of any new applications and systems;
    3) modifications or updates of the organization's policies and procedures;
    4) new or changed controls to resolve information security incidents and to improve security;
c) changes in supplier services to implement:
    1) changes and enhancement to networks;
    2) use of new technologies;
    3) adoption of new products or newer versions/releases;
    4) new development tools and environments;
    5) changes to physical location of service facilities;
    6) change of suppliers;
    7) sub-contracting to another supplier.



Center for Internet Security®

31 Tech Valley Drive
East Greenbush, New York 12061

518.266.3460

www.cisecurity.org

https://www.cisecurity.org/elections-resources/

CROWDSTRIKE

THREAT HUNTING WORKSHOP:
Hunting for Adversary Activity, Finding Evil, Eliminating the Threat

REGISTER NOW

Tuesday, October 16th at 12:00PM - 3:45PM EDT
510 Atlantic Ave | Boston, MA 02210

Join us for an intense adversary threat hunting program; learn the latest advanced adversary techniques and latest tradecraft. You will advance your threat hunting skills and methods and take your organization's ability to detect and hunt to the next level.

Through real world examples and demonstrations, our experts will show you new and existing techniques adversaries use, and how to proactively identify the earliest signs of active attacks.

KEY TAKEAWAYS:

- What is threat hunting, and why is it a critical discipline in today's security operations center?
- What are the latest tactics and techniques being used by modern adversaries?
- What data and tools do I need to effectively hunt for threats?
- How can I evolve threat hunting from an ad-hoc task to an operational part of my SOC?

Lunch and registration is from 12:00 PM – 1:00 PM. The workshop will start at 1:00 PM.

REGISTER NOW

Daniel J Cloutier

From: Thievon, Ed <Ed.Thievon@doit.nh.gov>
Sent: Friday, July 13, 2018 12:51 PM
To: Scott C. Caveney
Cc: Daniel J Cloutier
Subject: sos certs ready

Hi Scott,

I have two certificates for SOS ready for pick-up. blueexpress.sos.nh.gov and app.sos.nh.gov.

Do you have time today to retrieve them? If so, I'll set up the file exchange.

Ed Thievon
IT Manager, Web Support Division
Web Infrastructure
NH Department of Information Technology
603.230.3444
www.nh.gov/doit

Election Infrastructure Subsector
Government Coordinating Council
Charter

Article I – Official Designation

The official designation of this Council is the "Election Infrastructure Subsector Government Coordinating Council," hereinafter referred to as the "EIS GCC" or the "Council."

Article II – Mission and Purpose

The coordinating council enables local, state, and federal governments to share information and collaborate on best practices to mitigate and counter threats[1] to election infrastructure.

Specifically, the EIS GCC provides for interagency, intergovernmental, and cross-jurisdictional coordination within the Election Infrastructure Subsector and between this subsector and other sectors identified in Presidential Policy Directive/PPD-21 on "Critical Infrastructure Security and Resilience." The EIS GCC is composed of representatives from across various levels of government as appropriate to depict the operating landscape of the Election Infrastructure Subsector.

Article III – Objectives and Scope of Activity

The EIS GCC coordinates strategies, activities, and communications across governmental entities within the Election Infrastructure Subsector, and also reaches out across the national partnership structure defined in the current *National Infrastructure Protection Plan (NIPP)* and other policy documents in coordination with and in support of government and non-government subsector stakeholders. The scope of activity of the EIS GCC includes, but is not limited to:

- Coordinate with government and non-government subsector stakeholders to plan, implement, and execute the Nation's critical infrastructure security and resilience mission;
- Participate in planning efforts related to any revisions of the NIPP and the development and revision of Sector-Specific Plans (SSP);
- Promote interagency strategic communications coordination at the subsector level through partnership with DHS and other supporting agencies across various levels of government;
- Identify and support the information sharing capabilities and mechanisms that are most appropriate for State, Local, Tribal, Territorial (SLTT), Regional and private sector entities;
- Promote understanding and potential adoption of physical and cyber risk management processes, best practices, and use of innovative methods across the subsector;
- Enhance government information sharing across the subsector and promote multichannel public-private information sharing protocols and situational awareness;

[1] *See* "Assessing Russian Activities and Intentions in recent US Elections," Office of the Director of National Intelligence, January 6, 2017 *(available at:* https://www.dni.gov/files/documents/ICA_2017_01.pdf).

- Coordinate with government and non-government subsector stakeholders to set joint priorities and identify common risk management goals;
- Coordinate with government and non-government subsector stakeholders to develop processes for prioritizing and characterizing risk and incident management recommendations;
- Coordinate with government and non-government subsector stakeholders to identify knowledge gaps that warrant Research and Development (R&D) efforts.

Article IV – Membership

Member Representatives

EIS GCC membership is composed of government agencies and organizations representing government officials that own, operate or administer subsector physical or cyber assets, systems, and processes or have responsibility for supporting security and resilience of those assets, systems, and processes.

- Permanent membership resides with the agency or organization rather than the individual representatives.
- Each member agency or organization shall have primary and may have an alternate representatives to the EIS GCC.
- Primary agency representatives named to the EIS GCC are senior management level (Director or equivalent).

Members:

EIS GCC membership shall include the following Voting Members:

- Secretaries of State/Lieutenant Governors (where applicable) (x8)*
- State Senior Election Officials (x4, non-Secretaries of State)*
- Election Center – Local Government Election Officials (x3)
- International Association of Government Officials (iGO) – Local Government Election Officials (x3)
- U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection (x1)
- U.S. Election Assistance Commission (EAC) (x2) (Sitting Chair and Vice-Chair)
- Three State Election Officials and Three local election officials – (x6)** selected by the EAC's Federal Advisory Committees as listed below:
    - U.S. EAC Board of Advisors (x2) (one State Senior Election Official; one Local Government Election Official)
    - U.S. EAC Standards Board (x2) (one State Senior Election Official; one Local Government Election Official)
    - U.S. EAC Technical Guidelines Development Committee (x2) (one State Senior Election Official; one Local Government Election Official)

* Assigned/coordinated with appropriate supporting associations (NASS/NASED)

** The State and local election officials identified to serve on the GCC from the Election Assistance Commission's (EAC) Federal Advisory Committees shall serve on the GCC in their capacity as qualified election officials selected by each EAC advisory board, serving separately from their role in such advisory committees. In their role in the GCC, they do not represent the EAC's advisory committees, nor do they serve on the GCC in their private individual capacities.

Ex officio Members:

EIS GCC membership shall include the following Non-Voting Members:

- State, Local, Tribal, and Territorial Government Coordinating Council
- U.S. Election Assistance Commission
- U.S. Department of Commerce, National Institute of Standards and Technology
- U.S. Department of Defense, Federal Voting Assistance Program
- U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Cyber and Infrastructure Analysis
- U.S. Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity and Communications
- U.S. Department of Homeland Security, Office of Intelligence and Analysis
- U.S. Department of Justice, Federal Bureau of Investigation

EIS GCC membership may be expanded to include other government agencies and organizations, as well as other sector and cross-sector GCCs as additional non-voting members to provide relevant institutional knowledge, technical expertise, and administrative support, as determined by the membership of the EIS GCC. To expand EIS GCC membership it takes an affirmative vote of 2/3rds of the voting membership.

Member Alternate Representatives

Each voting and non-voting agency and organization of the EIS GCC may appoint one alternate representative to represent each member at EIS GCC activities.

- An alternate member representative casts the voting member's vote in the absence of the primary representative.
- Each voting and non-voting agency and organization is responsible for obtaining and maintaining the appropriate security clearance for its alternate representatives.

Article V – Governance, EIS GCC Leadership/Executive Committee

Governance

EIS GCC members will make decisions through a consultative and collaborative process, encourage the exchange of information and points of view, and strive for consensus. When a consensus cannot be achieved the EIS GCC will move to a vote. The EIS GCC recognizes that each member represents a government entity or organization with inherent legal authorities and parameters within which it must operate. At times, these authorities may restrict a member's ability to provide agreement on a decision or preclude the open dissemination of information. These inherent legal authorities must be clearly articulated by dissenting member when they are the basis for dissent and the inability to enter into consensus.

EIS GCC member representatives shall strive to faithfully represent the position of their government agencies or organizations; however, the EIS GCC recognizes that - in some cases - primary or alternate representatives may lack legal authority to act on behalf of its agency or organization. Therefore, the actions of individual members may not be binding on a government agency or organization.

EIS GCC Executive Committee

Due to the unique nature of the Election Infrastructure Subsector, National Protection and Programs Directorate (NPPD) SSA GCC Chair would like to conduct EIS GCC leadership matters using an "EIS GCC Executive Committee" (EIS EXCOM) model, which would include a representative number of member agencies or organizations from the EIS GCC. The EIS GCC Executive Committee would be comprised as follows:

- Chair - NPPD IP (x1)
- EAC Chair (x1)
- State-Secretary of State NASS President (x1)
- State-Senior State Election Official NASED President (x1)
- Local Government Election Official as determined by the Local members of the EIS GCC (x1)

Duties of EIS EXCOM

EIS GCC EXCOM shall have responsibility over the following areas:

- Location and agenda development;
- Monitoring and closure of issues and initiatives;
- Administrative and meeting support, including logistics and meeting minutes;
- Communications;
- Member and records management; and
- Maintenance of EIS GCC governance documents.
- When the EIS GCC conducts a meeting with non-government partners under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC), the Chair/EIS-EXCOM shall coordinate with the CIPAC Executive Secretariat/Designated Federal Officer to ensure compliance with CIPAC requirements.

Article VI – Meetings

Frequency of Meetings

The full membership of the EIS GCC will meet not fewer than two times each year in Washington, DC and/or in an alternative location as determined in consultation with EIS EXCOM. Full EIS GCC meetings will be scheduled with every attempt to provide ample notice to members. Telecon support will normally be provided.

Council meeting procedures will follow Robert's Rules of Order. EIS GCC members will make decisions through a consultative process, encouraging the exchange of information and points of view, and will strive for consensus.

Quorum

A duly constituted meeting of the EIS GCC shall require a quorum of more than half the number of voting members.

- Members must be personally present (including telephonically) or notify the EIS GCC EXCOM of their intention to participate and vote by remote means, in advance of a properly noticed meeting at which a vote is taken.
- The vote of a majority of the votes entitled to be cast by the voting members present at a meeting at which a quorum is present shall be necessary for the adoption of any matter voted upon by the members.

Principles of Participation

All EIS GCC members shall work towards the same goals and purpose of improving the security, preparedness, and resilience of Election Infrastructure. Discussion and deliberation processes must recognize and capitalize on each member's strengths, skills, and perspective. Results of EIS GCC discussions and deliberations must constitute a coherent voice made up of each member's contributions.

Article VII – Recordkeeping

The procedures for the handling, storage and disposition of EIS GCC records and other documentation are in accordance with DHS Federal Records Management policy, as well as directives and guidelines for the Election Infrastructure SSA.

Article VIII – Communications

The Election Infrastructure SSA will ensure a communication mechanism exists for sharing information among EIS GCC members.

Article IX – Working Groups

The EIS GCC shall form working groups as needed.

- Working groups shall be established when substantial investigation, research, or other tasks are required, which cannot be practicably achieved at regular EIS GCC sessions.
- All products of the working groups are meant to advise EIS GCC members on various issues and processes.
- Through its primary or alternate representatives, each member agency or organization may designate multiple individuals to serve on working groups.
- Working groups may be made up of any combination of EIS GCC member representatives and external participants serving as subject-matter experts.
- The EIS GCC will appoint a chairperson.
- Working group members will establish procedures consistent with this charter for the operation of the working group.
- Working group meetings may be held depending on need.
- Reports and recommendations from working groups will be presented at full EIS GCC meetings for member approval, as appropriate.

When the working group conducts a meeting with non-government partners under the auspices of CIPAC, the Chair/EI EXCOM shall coordinate with the CIPAC Executive Secretariat/Designated Federal Officer to ensure compliance with CIPAC requirements

Article X – Amendments

The EIS GCC may at any time amend this Charter by a 2/3rds vote of the voting members. The amended Charter shall be forwarded in a timely manner to the CIPAC Executive Secretariat for posting on the CIPAC public website.

Article XI – Duration

This Charter shall be in effect for two (2) years from the date of signing. If amended, the Charter shall be in effect from remainder of the initial two year period after the amendment is approved.

Article XII – Approval

The EIS GCC approved this Charter by vote of the attending members on October 14, 2017.

Public Comment of Meagan Wolfe

Interim Administrator
Wisconsin Elections Commission

U.S. Elections Assistance Commission
April 10, 2019

Version 2.0 of the Voluntary Voting System Guidelines
For Information Only: No Position Registered

Honorable Members:

Thank you Commissioners and staff of the EAC for hosting this meeting and for welcoming input from state and local election officials on the Voluntarily Voting Standards and Guidelines. Your willingness to receive input at this critical juncture is vital to the long-term success of the standards and certification process. I am Meagan Wolfe and it's my honor to serve as the Administrator for the State of Wisconsin Elections Commission and as the Chief Election Official for the State of Wisconsin. The Wisconsin Elections Commission has not taken a position on the VVSG, so I am presenting today's comments for information only.

Under the current EAC standards, voting systems cannot be updated quickly when they are patched, modernized, or otherwise changed. I urge you to consider state and local election officials' need to ensure that lack of quorum or ideological deadlock among EAC Commissioners does not affect our ability to provide our voters with modern, secure and usable voting equipment.

For many years, the Wisconsin Elections Commission and its predecessor agencies would not approve voting system that did not meet EAC certification and standards. Then, local election officials' strong desire to purchase new voting systems with modern features spurred a change in the process and ultimately the law. Local election officials experienced delays in the EAC process and found that the standards did not adequately reflect the requirements needed to ensure security in modern voting technology. Therefore, in 2015 a law was passed to eliminate the requirement that all voting systems approved for use in Wisconsin be accredited by the EAC and giving the state the ability to approve systems outside of the EAC certification process.

However, local election officials and state officials are still very hesitant to pursue equipment that has not been certified by EAC or without modern VVSG standards to guide our certification process. EAC certification and standards should be a foundation

on top of which our state standards are built, not an outdated roadblock we need to circumvent.

Election technology and security are dynamic. Standards that drive the development of election technology also need to be dynamic in order to keep pace. The tools we use to protect elections today are not the same tools that will be needed to protect elections tomorrow. Standards for our voting equipment are just one of many important tools we rely on as election officials. We must ensure that the principals and guidelines in place today are flexible enough to address current and future threats

As a first step, I urge the Commission to affirmatively vote to adopt the VVSG 2.0 principles and guidelines. This will solidify a vital tool for election officials to rely on as we undertake the important work of modernizing and updating our voting systems. I further urge you to plan for and allow for quick changes that may be needed. This can be accomplished by allowing the EAC Testing and Certification staff the authority to approve the requirements and test assertions, independent of the Commission. You can also further prepare the VVSG for the future by including a mechanism for approval absent a quorum or in the case of a deadlock of the Commission.

Unfortunately, election security needs do not evolve on an ideal timeline or under ideal circumstances. Contingency planning is essential to elections. As election officials, we never want to have to use our contingencies, but we must prepare strong contingencies to ensure strong elections. The VVSG should be held to this same standard. Let's work towards building resilient standards that will support secure elections, even under less than ideal circumstances. By adopting the recommendations of the Technical Guidelines Development Committee, the Standards Board, and the Board of Advisors, the EAC helps to ensure election officials have the tools we need to address the evolving challenges we may face in a timely manner.

Thank you again for the opportunity to speak with you. I appreciate your willingness to collect feedback and work towards the development of the best possible standards to help us accomplish our shared goal of administering secure, fair, and transparent elections.

Respectfully submitted,

Meagan Wolfe
Interim Administrator
Wisconsin Elections Commission
608-266-8005 / meagan.wolfe@wi.gov

REQUEST FOR APPLICATIONS

Policy Academy on Election Cybersecurity

IMPORTANT INFORMATION

Purpose: To maximize public confidence in elections by reducing technical risks to election systems and improving coordination between election officials and state cybersecurity leaders in the executive branch.

Opportunities Provided: Teams from five (5) competitively selected states will convene stakeholder workshops within their states to identify, refine, and/or implement promising practices in cybersecurity operations and communications directly related to elections.

Proposals Due:	8:00 PM ET, May 10, 2019
Informational Calls:	3:00 PM ET, April 5, 2019 2:00 PM ET, April 18, 2019 Conference Number: 888-858-6021 Conference Code: 202-624-5356
Selection Announcement:	Week of May 27, 2019
Project Period:	June 1, 2019 – December 1, 2019
Eligibility:	All eligible states, commonwealths, and territories.
NGA Contacts:	Maggie Brunner, Program Director, Cybersecurity and Communications, Homeland Security & Public Safety Division (202) 624-5364 or mbrunner@nga.org David Forscey, Senior Policy Analyst, Homeland Security & Public Safety Division (202) 624-5356 or dforscey@nga.org

PURPOSE

Election cybersecurity is a complex, long-term challenge that demands coordination across state and local governments. The National Governors Association Center for Best Practices (NGA Center)—in conjunction with technical support from the University of Southern California (USC)—is launching the *Policy Academy on Election Cybersecurity*, designed to facilitate intrastate dialogue and planning between election officials, governors' offices, and state cabinet agencies. This project will offer technical assistance to five states that have committed to improving intrastate coordination around election cybersecurity practices, policy, and planning. Combining expertise in state policy and technical research, the NGA Center will help interested states enhance interagency communication and cooperation, promote engagement by governors' offices, and

Application Checklist on Final Page

facilitate the development of statewide response plans for attacks on election infrastructure. Technical assistance offerings include facilitated strategic planning, policy design and development, state comparative analysis, document drafting, access to subject matter experts, and general capacity building.

Supporting organizations for the Policy Academy on Election Cybersecurity *include the National Association of State Election Directors and the National Association of Secretaries of State. Funding is provided by the Democracy Fund.*

BACKGROUND

Election officials have worked diligently against malicious attempts to undermine public trust in elections. Well before the 2016 elections, these efforts included important steps to address security vulnerabilities in voting systems, election management systems, and the procedures that rely on those systems.

Since 2016, the elections community has devoted unprecedented time, attention, and funding into cybersecurity controls designed to reduce risk. Driving these concerted efforts is evidence that foreign governments possess the means and intent to influence elections in the United States.

Notwithstanding geopolitics, other developments further underscore the need to prioritize election cybersecurity. First, in recent years, highly sophisticated hacking tools have become widely available, empowering novice attackers. Second, media reports have increased public concern about the security of elections and even highlighted opportunities for election interference. Third, increased public reliance on social networks for information magnifies the risks posed by isolated security events. For example, a single incident, real or perceived, affecting one voting or election system in one jurisdiction—reported by news media and amplified through social media—could undermine public confidence in broader election outcomes. In short, election practitioners confront a long-term struggle against a diverse set of potential attackers, who are increasingly capable, with a range of motivations, and who cannot all be deterred with the same tools.

Addressing this threat demands a whole-of-government approach that integrates all relevant cybersecurity resources and planning. This requires coordination across independent agencies. In many states, elections are managed by an independently elected constitutional officer who does not report to the governor. Yet significant cybersecurity expertise and resources can be found in departments and agencies subordinate to the governor. State information technology, homeland security, and public safety departments have expertise and capabilities that can boost the capacity of election officials to defend voting systems and election systems. Many National Guard cyber units comprise experts who work full-time in world-class technology companies. In dozens of states, cybersecurity leaders under the governor are collaborating through formal and informal governance bodies to write statewide cybersecurity strategies and disruption response plans that will guide cybersecurity investment and assistance.

A series of obstacles are limiting coordination between the election community and governors' cybersecurity leaders. Although the 2016 elections advanced a dialogue between election officials and governors' advisors, decades of siloed operations have deprived all stakeholders of the personal relationships and mutual understanding that are critical for long-term collaboration. Election officials are often left out of statewide strategies and plans. Election offices seeking help from the National Guard may lack support from the governors' office to request Guard resources. Governors' offices and state cabinet leaders may not always know what election officials need, from funding and technical assistance to coordinated public messaging.

POLICY ACADEMY DESCRIPTION

In recognition of the above challenges, the NGA Center, in a partnership with the University of Southern California, is launching the *Policy Academy on Election Cybersecurity*. This initiative is designed to help states maximize public confidence by fostering long-term coordination between election officials, governors' offices, and state cybersecurity leaders.

An NGA policy academy is a highly collaborative, team-based process for helping a select number of states develop and implement action plans that address complex public policy challenges. Participating states receive guidance and technical assistance (e.g., facilitated workshops, policy research, written products) from NGA Center staff and, as appropriate, access to subject matter experts from the private sector, research organizations, academia, and the federal government. A policy academy provides a forcing mechanism that focuses the time and attention of stakeholder groups that can prove difficult to convene under normal circumstances. The strategies and policies developed by participating states are intended to catalyze wider adoption of promising practices across the United States. The *Policy Academy on Election Cybersecurity* will benefit from direct research support provided by staff and faculty from the University of Southern California. ***Note: This project is not an academic study, and no state-specific findings or conclusions will be published or otherwise shared or discussed publicly without the express consent of participating states and other relevant stakeholders.***

Key Benefits

The primary activities of the *Policy Academy on Election Cybersecurity* include (a) technical assistance provided by NGA Center staff and appropriate subject matter experts; (b) a two-day multidisciplinary, in-state workshop to convene election officials and state cybersecurity leaders to create action plans; and (c) limited funding to cover travel costs for stakeholders. These activities will support goals that states choose to prioritize. Examples of appropriate state goals include:

- Integrating the needs of election officials into statewide strategies and investment plans;
- Engaging new gubernatorial administrations and building support for past and future election cybersecurity initiatives;
- Identifying and/or communicating election cybersecurity needs, corresponding budgets, and legislative strategies;
- Creating election cybersecurity priorities, policies, and plans for National Guard units;
- Leveraging all existing state, federal and/or local resources to scale training and assistance for local election offices (e.g., shared services contracts);
- Creating a statewide communications strategy that coordinates election cybersecurity messaging across relevant state and local offices;
- Integrating election offices with state fusion centers or security operations centers, or establishing a dedicated center for election cybersecurity activities;
- Identifying gaps in state law and potential solutions;
- Facilitating conversations with critical infrastructure owners and operators (e.g., internet service providers or utilities).

State Team Responsibilities

The Policy Academy will require preparation from state attendees before the in-state workshop, active team participation throughout the policy academy process, and a strong commitment to implementing action plans. Specifically, participating states are required to:

- *Participate in scheduled conference calls.* Following state selection, the NGA Center will host conference calls with participating states to orient them to the Policy Academy and outline next steps, including policy academy preparatory work and meetings, available technical assistance and resources from NGA Center staff and other experts, and site visits by NGA Center staff. Monthly conference calls will maintain coordination until the in-state workshop. Conference calls may continue on an as-needed basis for states who request additional virtual technical assistance following the workshop.
- *Develop state needs assessment and gap analysis.* Through initial conferences calls and other preparatory work, the NGA Center will complete a confidential gap analysis and needs assessment for each state. The gap analysis and needs assessment will provide team members with a better understanding of their state's challenges and serve as a baseline for evaluating outcomes of the policy academy.
- *Convene an in-state workshop.* The in-state workshop provides the core benefit of the Policy Academy process. Staff from the NGA Center will conduct a two-day visit in each state to help teams identify and/or implement action plans to achieve the objectives outlined in the Policy Academy application. Active participation by the entire Policy Academy team is required.
- *Complete evaluation survey and lessons learned report.* After the Policy Academy, participating states will be asked to complete a survey for the NGA Center on the work they accomplished during the project. State responses will be used for evaluation purposes and, with the state's consent, will be included in a public report on the lessons learned during the Policy Academy, to be disseminated to all other states and territories.

POLICY ACADEMY APPLICATION PROCESS

(SEE APPLICATION CHECKLIST ON LAST PAGE)

Step 1: Secure Commitment from the Governor and Chief Election Official(s)

The goal of this Policy Academy is to improve intrastate coordination between governors' offices, state cabinet agencies, and election offices. Interested state teams should secure approval from the governor and the chief election official of the same state. Each team will be asked to submit a joint letter or separate letters of commitment from the governor and chief election official. (See Step 3.)

Step 2: Identify a Policy Academy Team

Each interested state should assemble a high-level multidisciplinary "core" team of state representatives, plus a larger, more comprehensive team. The core team will (a) manage the full team; (b) prioritize state objectives; and (c) lead coordination with the NGA Center and other relevant support organizations.

Team leads: The core team will be led by two state officials, one selected by the governor's office, and one selected by the chief state election official(s) (or by the designee of the chief state election official).

Application Checklist on Final Page

Core team: The team leads will designate the rest of the core team, comprising a mix of relevant representatives from each respective branch of government. The core team must include a minimum of six (6) state officials, including the team leads; each state is free to determine the appropriate size of its core team beyond the minimum. Two possible examples of core teams are:

- Example 1: Adjutant General, statewide Chief Information Officer, statewide Homeland Security Advisor, Secretary of State, Election Director, and Chief Information Officer for the statewide election office.
- Example 2: Head of the Department of Motor Vehicles, statewide Chief Information Security Officer, Commissioner of Public Safety, two county Election Directors, and the statewide Elections Commissioner.

Full team: The core team will designate a larger team that can include not only state officials, but also non-state and local actors, such as local election officials, academic advisors, nonprofit representatives, and others. *The full team does not need to be described in the written application.*

Step 3: Draft the Application Narrative. Formal applications to participate in the Policy Academy cannot exceed six (6) pages and must include:

(1) *Letter(s) of application from the governor and the chief election official:* The letter or letters of application, co-signed by the governor and chief election official (or, if using separate letters, signed by each), should briefly articulate the state's interest in and desired outcomes related to this project, and how those outcomes fit within the state's commitment to election security. The letter(s) must designate the two team leads who will direct the team's efforts with the NGA Center. The letter(s) will *not* count against the six-page limit.

(2) *Proposal narrative:* The proposal narrative should not exceed six-pages single-spaced, 11-point font, 1" margins. **Please see the final page of this document for evaluation criteria that offer a guide for narrative content**.

Step 4: Submit the Application. All proposals must be received by **5:00 PM PST on May 10, 2019**. Only one application per state will be considered, and it must be transmitted by a state employee. Prior to submission, please assemble the proposal materials into a single PDF document. **Please email the proposal to Maggie Brunner at mbrunner@nga.org.** NGA will confirm receipt within one business day.

POLICY ACADEMY TIMELINE

The following is a tentative schedule for the academy:

3:00 PM ET, April 5, 2019 Number: 888-858-6021 Code: 202-624-5356	**1st Bidders' Call** The NGA Center will host an optional conference call for all interested states to answer questions about the Request for Application (RFA) process, proposal content, submission requirements, or other issues.
2:00 PM ET, April 18, 2019 Number: 888-858-6021 Code: 202-624-5356	**2nd Bidders' Call**

Application Checklist on Final Page

	The NGA Center will host an optional conference call for all interested states to answer questions about the RFA process, proposal content, submission requirements, or other issues.
5:00 PM PST, May 10, 2019	**Proposals Due**
Week of May 27, 2019	**State Selection Announcement** The NGA Center will notify states of their application status and issue a press release announcing winning states.
June 2019 – December 2019	**In-State Workshops** Objectives: • Engage state team in planning process • Refine initial recommendations • Develop strategic action plan for implementing recommendations
Ongoing	Monthly conference calls and webinars with Policy Academy staff and other participating states.

SELECTION CRITERIA **(Total points possible = 100 pts)**

Note: States can use these criteria in drafting the narrative portion of their application.

Category	Description	Value
Description of the Problem	• Applicants should describe current efforts to secure election and voting infrastructure at the state and local levels. • Applicants should explain limitations of the state's current approach that may be relevant.	20 points
Anticipated Benefits and Potential Outcomes	• Applicants should explain how improving coordination between election offices and other state cybersecurity offices will help the state address identified challenges and improve their overall efforts to secure elections. They should articulate a clear "business case" for how proposed changes will help them achieve state goals. • Applicants must demonstrate that the state is poised to make significant progress toward improving their statewide efforts to secure election infrastructure. For example, is there buy-in from key political leaders, agency leadership, local government, and communities? If not, will the Policy Academy help to solve that? • Applicants should identify specific outcomes they hope to achieve by the end of the Policy Academy. *Applicants should focus on activities that support election cybersecurity. This Policy Academy will not focus on information operations.*	30 points
Obstacles to Implementing Solutions	***This section does not count toward the six-page limit.***	20 points

Application Checklist on Final Page

	• Applicants should identify any potential obstacles that could derail development or implementation of their goals. Further, they should explain how they might address those challenges. *For states that are undergoing a gubernatorial or chief election official transition, please address how you will pursue completion of Policy Academy goals and activities through that transition.*	
Evaluation Plan	• Applicants must identify a plan that ties goals and objectives to tangible metrics. • Describe what those metrics are and how they would be measured. ***This section does not count toward the six-page limit.***	10 points

Team Composition and Member Roles	***This section does not count toward the six-page limit.***
	
	• **Team Leads**: The governor and chief election official must each designate a separate representative from their branch to co-lead the state's Policy Academy project.
	• **Core Team**: Each state must assemble a multi-disciplinary "core" team comprising of a minimum of six (6) state leaders (including the team leads) with demonstrated equities in elections, cybersecurity, homeland security, and/or emergency preparedness. Applicants should briefly discuss the rationale behind the core team composition and the roles and responsibilities each member will take on in support of achieving team objectives.
	  ○ Please provide each core team member's name, title, work address, phone, and e-mail address.
	  ○ *Note: resumes or curriculum vitae are not required.*
	• **Full Team:** States can identify additional members of the full team, above and beyond the core team. This can be a much broader and more diverse group, and can include state, local, and non-governmental partners, to consult with during the Policy Academy and to convene during the state's two-day workshop.
	  ○ Note: For purposes of the full team members, simply listing agencies/affiliations, rather than specific individuals, is sufficient.
	
	This section does not count toward the six-page limit.
		20 points

Disclaimers

This request for application is not binding on the NGA Center, nor does it constitute a contractual offer. Without limiting the foregoing, the NGA Center reserves the right, in its sole discretion, to reject any or all applications; to modify, supplement, or cancel the RFA; to waive any deviation from the RFA; to negotiate regarding any application; and to negotiate final terms and conditions that may differ from those stated in the RFA. Under no circumstances shall NGA Center be liable for any costs incurred by any person in connection with the preparation and submission of a response to this RFA.

Application Checklist on Final Page

Policy Academy on Election Cybersecurity
Application Checklist

Application Process

- ☐ Consult with Governor's Office and Chief Election Official Regarding Application Process
- ☐ Identify Team Leads
- ☐ Identify Core Team
- ☐ Prepare Narrative Description (maximum of six (6) pages single-spaced)
- ☐ Email Application in PDF Format to Maggie Brunner at mbrunner@nga.org **before 5:00 PM PST on May 10, 2019**.

Application Contents

- ☐ Letter(s) of Application from Governor and Chief Election Official
- ☐ Narrative Description (Maximum length of six (6) pages, single-spaced)
  - Description of the Problem
  - Anticipated Benefits and Potential Outcomes
  - Obstacles to Implementing Solutions
  - Evaluation Plan (does not count toward the page limit)
  - Team Composition (does not count toward the page limit)
    - Team Leads
    - Core Team
    - Full Team (optional—members of the full team can be identified after the Policy Academy application has been submitted)

Madam Chair and EAC Commissioners, my name is Rob Rock, Director of Elections for Rhode Island Secretary of State Nellie Gorbea. Thank you for the opportunity to present comments on behalf of Secretary Gorbea regarding a vital issue facing the EAC.

Before I begin, I would like to acknowledge the hard work and dedication of those who helped craft the Voluntary Voting System Guidelines, version 2.0. To those state and local election officials, technology and accessibility experts, voting system vendors, and federal partners including representatives from the National Institute of Standards and Technology, and the EAC itself – thank you for your hard work and dedication.

The principles and guidelines of the VVSG 2.0 are an important part of ensuring that our nation's voting systems are properly tested and certified. I believe these principles and guidelines should require an affirmative vote of the EAC Commissioners to be adopted.

However, the requirements and test assertions of the system should be the responsibility of EAC Testing and Certification staff -- not subject to a vote by the Commission. At the very least, there should be a mechanism by which future iterations of the VVSG can move forward in the absence of a quorum, or in the case of a deadlocked vote by the Commission. This would ensure that our future voting systems receive proper vetting before being released.

It is imperative that we have a testing and certification process that can respond to the ever-evolving technology and cybersecurity environment, so voters can have faith in the integrity of our election systems.

I have publicly stated in the past how vital the EAC is to state and local election officials. The EAC provided invaluable assistance with Rhode Island's procurement of voting equipment and e-poll books. The staff provides helpful and timely expertise, and your website is an incredible source of information to states as we strive to stay up to date with a constantly evolving technology landscape.

On behalf of Secretary Gorbea, I urge you to continue your strong track record of being an elections partner by allowing the Voluntary Voting System Guidelines to move forward as recommended by the Technical Guidelines Development Committee, the Standards Board, and the Board of Advisors. Thank you.

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, July 10, 2018 2:21 PM
To: Anthony Stevens; David Scanlan
Subject: Re: EIS-GCC - All Day Friday
Attachments: govt-facilities-election-infrastructure-subsector-gcc-charter-2017-508.pdf; govt-facilities-sector-gcc-charter-2017-508.pdf

Dave & Anthony,

Apparently this is a real committee of several individuals. It is possible this will be an open meeting where others can attend and listen. I don't know. Here is a link to the proposed first meeting: https://www.dhs.gov/news/2017/10/14/dhs-and-partners-convene-first-election-infrastructure-coordinating-council

Attached are two documents of the charter - one appears to be an update?

Thanks,

Dan

Daniel J. Cloutier
Assistant Secretary of State

9 Ratification Way - Concord, NH
Tel: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens
Sent: Tuesday, July 10, 2018 12:54 PM
To: Daniel J Cloutier
Subject: EIS-GCC - All Day Friday

Election Infrastructure Subsector Government Coordinating Council, all day Friday.

https://www.nass.org/events/nass-2018-summer-conference#agenda

Anthony Stevens
Assistant Secretary of State
71 S. Fruit St.
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Monday, April 22, 2019 11:53 AM
To: Daniel J Cloutier
Subject: FW: Update, 4/19
Attachments: Tabletop the Vote 2018 National Election Cyber Tabletop Exercise AAR_v00 approved.pdf; Standards Board Public Comment[2].docx; MW Testimony US-EAC VVSG 04-10-2019[1].docx; Request for Applications - NGA Policy Academy on Election Cybersecurity.pdf

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Amy Cohen <acohen@nased.org>
Sent: Friday, April 19, 2019 3:29 PM
To: Amy Cohen <acohen@nased.org>
Subject: Update, 4/19

Hi all,

Happy Friday!

- In case you've been completely off the grid for the last 24 hours or you've been watching the Beyoncé documentary on repeat, the Mueller report was released (volume 1 and volume 2). The pages related to election administration are pages 50-51 of volume 1.
- As you know, Kirstjen Nielsen is no longer the Secretary of Homeland Security; Kevin McAleenan is the Acting Secretary for DHS. Election security remains a priority for the agency and we can expect the same level of commitment that we had under Former Secretary Nielsen.
- Attached is an after-action report from last year's Virtual TTX. As a reminder, this year's Virtual TTX will be June 18, 19, and 20. An invitation will be coming soon, hopefully next week.
- Earlier today, Senator Klobuchar (D-MN) and 30 other senators sent a letter to the Senate Appropriations Subcommittee on Financial Services and General Government to increase funding to the EAC (funding was cut in the FY20 budget) and provide an additional $250 million in grants for state and local election offices. It does also sound like we could see something around a steady funding stream in the coming weeks/months, so stay tuned on that.
- Attached please find the testimony that Rob Rock (Rhode Island) and Meagan Wolfe (Wisconsin) delivered last week at the public hearing in Memphis prior to the EAC Standards Board meeting. Mark Goins (Tennessee) also testified; his main point "was that the process for developing and approving the VVSG is too slow. Within the confines of federal law, the new testing guidelines and assertions need to be implemented as soon as possible." There will be another public hearing on April 23 from 3-6pm MT, held in conjunction with the Board of Advisors meeting in Salt Lake City, UT. That hearing will be livestreamed on eac.gov.

- A reminder that the public comment period for the VVSG 2.0 ends on May 29 at 4pm ET. The NASED Board is working on a comment and will circulate it to all of you as soon as we can. The VVSG 2.0 document is available here.
- A reminder about the National Governor's Association application for its Policy Academy on Election Cybersecurity (attached). The goal is to work with five states to improve coordination between election offices and the executive branch. If you have any questions about the RFA or the project, please contact Maggie Brunner (mbrunner@nga.org; 202-624-5364). Applications are due by **8pm ET on May 10, 2019**. Both NASS and NASED worked with NGA on the RFA itself and are helping to make sure this project is valuable for state election offices.

Have a lovely weekend!

Amy

Amy Cohen
Executive Director
National Association of State Election Directors
Phone: 240-801-6029
Mobile: 203-536-3660
Follow us on Twitter @NASEDorg and on Facebook!

Date	Time	City/Town	Facility
Friday, August 3, 2018	9:00 – 11:30 AM HAVA 6:00 AM	Newport	Newport Middle High School - Cafeteria 245 North Main St., Newport Colleen
Monday, August 6, 2018	11:30 AM – 2 PM HAVA 6:45 AM	Colebrook	Colebrook Court Room, Town Hall 17 Bridge St., Colebrook Colleen
Monday, August 6, 2018	6:00 – 8:30 PM	Berlin	White Mountain Community College Class Room #100, Main Floor 2020 Riverside Dr., Berlin Colleen
Wednesday, August 8, 2018	9:00 – 11:30 AM HAVA 6:00 AM	Portsmouth	Portsmouth High School Library, Little Theater 50 Andrew Jarvis Drive, Portsmouth Colleen & Debbie
Friday, August 10, 2018	9:00 – 11:30 AM HAVA 6:00 AM	Keene	Michael E.J. Blastos Community Room 400 Marlboro St., Keene Colleen & Debbie
Tuesday, August 14, 2018	12:00 – 2:30 PM HAVA 9:00 AM	Wolfeboro	Great Hall/Wolfeboro Town Hall 84 S Main St., Wolfeboro Colleen & Sheila
Tuesday, August 14, 2018	6:00 – 8:30 PM	Conway	Conway Village Fire Station 97 Main St., Conway Colleen & Sheila
Thursday, August 16, 2018	9:00 – 11:30 AM HAVA 6:00 AM	Brentwood	Brentwood Community Center 190 Route 125, Brentwood Colleen & Debbie
Saturday, August 18, 2018	9:00 – 11:30 AM HAVA 6:00 AM	Campton	Campton Municipal Building 10 Gearty Way, Campton Sheila
Tuesday, August 21, 2018	9:00 – 11:30 AM HAVA 6:15 AM	Franklin	Franklin Opera House Sheila 316 Central St., Franklin, (parking in rear)
Thursday, August 23, 2018	9:00 – 11:30 AM HAVA 5:30 AM	Rindge	Rindge Meeting House 6 Payson Hill Road, Rindge Debbie
Saturday, August 25, 2018	9:00 – 11:30 AM HAVA 6:30 AM	Hopkinton	Hopkinton High School Auditorium 297 Park Ave., Contoocook Sheila
Tuesday, August 28, 2018	6:00 – 8:30 PM HAVA 3:00 PM	Atkinson	Atkinson Country Club, Banquet Room 85 Country Club Drive, Atkinson Debbie
Thursday, August 30, 2018	1:00 – 3:30 PM HAVA 9:00 AM	Lancaster	Lancaster Town Hall Auditorium Sheila 25 Main St., Lancaster (parking next door)
Friday, August 31, 2018	12:00 – 2:30 PM HAVA 9:15 AM	Nashua	Nashua High School North - Auditorium 8 Titan Way, Nashua Debbie
Wednesday, September 5, 2018	9:00 – 11:30 AM HAVA 5:30 AM	Piermont	Piermont Fire Station – Across the street from the school 130 Route 10, Piermont Sheila
Thursday, September 6, 2018	9:00 – 11:30 AM HAVA 5:45 AM	Rochester	Rochester Community Center, Sheila 150 Wakefield St./Community Way Chestnut Hill Road Entrance, Rochester

Daniel J Cloutier

From: NHVotes <NHVotes@sos.nh.gov>
Sent: Wednesday, August 8, 2018 9:50 AM
To: Daniel J Cloutier
Subject: E-mail Message from nhvotes
Attachments: 20180808095007.pdf

```
This is an E-mail message.
Please open the attached file.
  Sent from       : "NHVotes" <NHVotes@sos.nh.gov>
                    603-271-8242
  Number of pages : 1
  Date            : Wed, 8 Aug 2018 09:50:07 -0400
```

STATEMENT OF WORK

Client	NH Secretary of State	**CR No.**	2018 - ~~001~~ 002
Project Name	NH CVRS	**Project No.**	60042
Project Manager	Keval Patel	**Client Contact**	Colleen McCormack
Requested By	Elections Division	**Request Date**	05/01/2018
Client Approver	Anthony Stevens	**Date Submitted**	05/15/2018
Priority (H, M, L)	H	**Client Reply Date**	

Description of Change

1. Two Factor Authentication

New Hampshire Secretary of State's Elections Division has requested PCC to implement two-factor authentication to enhance the security of the SVRS.

The proposed solution is a process whereby an authorized user attempting to login from any computer would receive a challenge and be required to input an additional code (security code). The code would be sent to a pre-defined email address or cell phone number. This would be entered in addition to the user id and password. And access to SVRS by two-factor authentication is managed by the various configurable fields available to the authorized user.

To implement this new functionality for added security, the following changes need to be made to SVRS.

1. All **'Maintain Users'** screens will have an additional field to collect user's email address and cell phone number.
   - Add a new field to enter the user's email address number labelled **'Email Address'.**
   - Add a new field to enter the user's cell phone number labelled **'Cell Phone'**. This is not a mandatory field but if the user profile has the cell phone number then the user can receive the authentication code to either the email address or the cell phone.

2. My Homepage to add cell phone field to display.
   - The **'My Homepage'** screen will be modified to display the user's cell phone number entered in the **'Maintain Users'** screen.

3. If the user needs to update their Email Address and/or Cell Phone number, they will need to contact the authorized user and provide the updated information who in turn will update the user profile.

4. A new screen will be provided for the authorized user to manage the various configurable parameters of the two-factor authentication. This will provide flexibility and control to the authorized user to manage the settings easily and efficiently.
   - The authorized user can manage the authentication methods to be available for the users by turning them on and off. The authorized user can turn on either only the email authentication or only the cell phone authentication or both. The authorized user can turn 'Off' the complete Two-factor Authentication functionality.
   - The system will provide an option for the authorized user to control whether the 'Remember this browser' feature should be turned on or off.
   - If the 'Remember this browser' is turned on and if any user has this selected the authorized user can reset and force the users to go through the authentication process again. The system will provide the option to reset this every 30, 60 or 90 days.
   - The authorized user can also set the different times of the day they would want the users to go through this authentication process.
   - A section to manage the IP Addresses that will be not be required to go through this Two-factor Authentication process will be provided for the authorized user. The user can enter and manage the IP Address ranges that should be excluded from the authentication process.

- An option for the authorized user to do a systemwide reset and force the users to go through the Two-factor Authentication the next time they login will also be available.
- The authorized user can choose the length of time (in minutes) the authentication code is valid.
- The authorized user can choose the length of time (in minutes) the verification link is valid.
- The authorized user can set the number times the user can enter the code incorrectly before being locked from generating the authentication code.

5. In addition, the system will provide option for the authorized user to manage two-factor authentication at the user level. The authorized user can enable / disable two-factor authentication at an individual user level to have greater flexibility.

6. An additional screen will be provided at the login stating that the user needs to enter additional code to login to SVRS and requesting the user to select if authentication code be sent to email or cell phone. If the user does not have a cell phone number on the profile, then the user will have only email as an option to receive the authentication code. If both email address and cell phone number are available on the profile, then the system will display email and cell phone as options to receive the authentication code.
   - All the users except the ones whose IP Address is listed to be not considered for this authentication or the roles not enabled for Two-factor Authentication or the towns or users not enabled for two-factor authentication the system will display a secondary screen asking the user how they would wish to receive the authentication code.
   - Based on the option selected the system will send an authentication code and the user needs to enter this code in the next screen and if the correct code is entered the system will navigate to the SVRS Reminders screen.
   - If for some reason the user does not receive the authentication code, then the user can request for the code to be sent again from this screen.
   - If an incorrect authentication code is entered the authentication fails.
   - The validity of the code will be set by the authorized user.

7. An additional checkbox on this login screen asking if the user would like SVRS to remember this computer.
   - On the secondary screen the system will provide an option asking the user if they would like SVRS to remember the browser so that they do not have to go through same authentication process again the next time they login. If the user selects this checkbox then SVRS will not ask for this authentication the next time when the user access SVRS from this browser. If the user does not select this option, then SVRS will ask for this authentication every time the user access SVRS until the option to remember the browser is selected.

8. All users at next login would be required to have their email address and/or cell phone number on their profile depending on which information is missing.

9. Cell Phone Number and Email Address Verification.
   - Additional functionality to verify the email address and/or the cell phone number associated with the user's profile is valid and indeed the user's will be provided.
   - When the user logs in a secondary screen will be provided with the email address and cell phone number on the user profile and an option to verify them individually. On submitting the request, the system will send a link to the user's email address and/or cell phone and asking the user to complete the process by clicking on the link.
   - Once the user clicks the click before it expires the user's email address and/or cell phone will be verified.
   - If the user does not receive the verification link, then the user can contact the authorized user to check if they entered the information incorrectly or if the user provided the information incorrectly and correct it.

Other Items

- **The module will be hosted on the same instance as the NH ElectioNet Production application.**
- **Email Notifications will be managed from the current Amazon SES.**
- **SMS Service will be handled by the Amazon SNS.**

Delivery Schedule

Estimated Completion Date is on or before **July 27, 2018** in UAT.

#	Description	Start Date	End Date
1.	Interface Requirement /JAD / FRD	May 21, 2018	May 25, 2018
2.	Interface Development	May 24, 2018	July 13, 2018
3.	System and Unit Testing	June 2, 2018	June 13, 2018
4.	UAT & Deployment	June 16, 2018	July 27, 2018
5.	Go Live	TBD	

Phase and Cost Details

Description	Estimated Hours	Rate/hr.	Total
PM & BA	120	$92.00	$11,040.00
Developer	600	$92.00	$55,200.00
Testing & Deployment	160	$92.00	$14,720.00
Total Hours	**880**	**Total Amount**	**$80,960.00**

Terms and Conditions

- The above estimates are based on the agreed upon requirements determined by consultation between PCC and NH SOS. Any unforeseen extra time required to accomplish any of the above tasks shall be communicated to the client and would require approval for the additional time requested.
- These estimates are based on the needs defined by NH SOS.
- The total cost will be based on the above resource usage.

PCC Approval

Signature [signature] Title CTO Date 6/11/2018

Client Approval

Accept [X] Disapprove [ ]

Signature [signature] Title DEPUTY SECRETARY OF STATE Date 6/8/18

Comments [signature] 6/8/18

STATEMENT OF WORK

Client	NH Secretary of State	**CR No.**	2018 - ~~001~~ 002
Project Name	NH CVRS	**Project No.**	60042
Project Manager	Keval Patel	**Client Contact**	Colleen McCormack
Requested By	Elections Division	**Request Date**	05/01/2018
Client Approver	Anthony Stevens	**Date Submitted**	05/15/2018
Priority (H, M, L)	H	**Client Reply Date**	

Description of Change

1. Two Factor Authentication

New Hampshire Secretary of State's Elections Division has requested PCC to implement two-factor authentication to enhance the security of the SVRS.

The proposed solution is a process whereby an authorized user attempting to login from any computer would receive a challenge and be required to input an additional code (security code). The code would be sent to a pre-defined email address or cell phone number. This would be entered in addition to the user id and password. And access to SVRS by two-factor authentication is managed by the various configurable fields available to the authorized user.

To implement this new functionality for added security, the following changes need to be made to SVRS.

1. All **'Maintain Users'** screens will have an additional field to collect user's email address and cell phone number.
   - Add a new field to enter the user's email address number labelled **'Email Address'.**
   - Add a new field to enter the user's cell phone number labelled **'Cell Phone'**. This is not a mandatory field but if the user profile has the cell phone number then the user can receive the authentication code to either the email address or the cell phone.

2. My Homepage to add cell phone field to display.
   - The **'My Homepage'** screen will be modified to display the user's cell phone number entered in the **'Maintain Users'** screen.

3. If the user needs to update their Email Address and/or Cell Phone number, they will need to contact the authorized user and provide the updated information who in turn will update the user profile.

4. A new screen will be provided for the authorized user to manage the various configurable parameters of the two-factor authentication. This will provide flexibility and control to the authorized user to manage the settings easily and efficiently.
   - The authorized user can manage the authentication methods to be available for the users by turning them on and off. The authorized user can turn on either only the email authentication or only the cell phone authentication or both. The authorized user can turn 'Off' the complete Two-factor Authentication functionality.
   - The system will provide an option for the authorized user to control whether the 'Remember this browser' feature should be turned on or off.
   - If the 'Remember this browser' is turned on and if any user has this selected the authorized user can reset and force the users to go through the authentication process again. The system will provide the option to reset this every 30, 60 or 90 days.
   - The authorized user can also set the different times of the day they would want the users to go through this authentication process.
   - A section to manage the IP Addresses that will be not be required to go through this Two-factor Authentication process will be provided for the authorized user. The user can enter and manage the IP Address ranges that should be excluded from the authentication process.

- An option for the authorized user to do a systemwide reset and force the users to go through the Two-factor Authentication the next time they login will also be available.
- The authorized user can choose the length of time (in minutes) the authentication code is valid.
- The authorized user can choose the length of time (in minutes) the verification link is valid.
- The authorized user can set the number times the user can enter the code incorrectly before being locked from generating the authentication code.

5. In addition, the system will provide option for the authorized user to manage two-factor authentication at the user level. The authorized user can enable / disable two-factor authentication at an individual user level to have greater flexibility.

6. An additional screen will be provided at the login stating that the user needs to enter additional code to login to SVRS and requesting the user to select if authentication code be sent to email or cell phone. If the user does not have a cell phone number on the profile, then the user will have only email as an option to receive the authentication code. If both email address and cell phone number are available on the profile, then the system will display email and cell phone as options to receive the authentication code.
   - All the users except the ones whose IP Address is listed to be not considered for this authentication or the roles not enabled for Two-factor Authentication or the towns or users not enabled for two-factor authentication the system will display a secondary screen asking the user how they would wish to receive the authentication code.
   - Based on the option selected the system will send an authentication code and the user needs to enter this code in the next screen and if the correct code is entered the system will navigate to the SVRS Reminders screen.
   - If for some reason the user does not receive the authentication code, then the user can request for the code to be sent again from this screen.
   - If an incorrect authentication code is entered the authentication fails.
   - The validity of the code will be set by the authorized user.

7. An additional checkbox on this login screen asking if the user would like SVRS to remember this computer.
   - On the secondary screen the system will provide an option asking the user if they would like SVRS to remember the browser so that they do not have to go through same authentication process again the next time they login. If the user selects this checkbox then SVRS will not ask for this authentication the next time when the user access SVRS from this browser. If the user does not select this option, then SVRS will ask for this authentication every time the user access SVRS until the option to remember the browser is selected.

8. All users at next login would be required to have their email address and/or cell phone number on their profile depending on which information is missing.

9. Cell Phone Number and Email Address Verification.
   - Additional functionality to verify the email address and/or the cell phone number associated with the user's profile is valid and indeed the user's will be provided.
   - When the user logs in a secondary screen will be provided with the email address and cell phone number on the user profile and an option to verify them individually. On submitting the request, the system will send a link to the user's email address and/or cell phone and asking the user to complete the process by clicking on the link.
   - Once the user clicks the click before it expires the user's email address and/or cell phone will be verified.
   - If the user does not receive the verification link, then the user can contact the authorized user to check if they entered the information incorrectly or if the user provided the information incorrectly and correct it.

Other Items

- **The module will be hosted on the same instance as the NH ElectioNet Production application.**
- **Email Notifications will be managed from the current Amazon SES.**
- **SMS Service will be handled by the Amazon SNS.**

Delivery Schedule

Estimated Completion Date is on or before **July 27, 2018** in UAT.

#	Description	Start Date	End Date
1.	Interface Requirement /JAD / FRD	May 21, 2018	May 25, 2018
2.	Interface Development	May 24, 2018	July 13, 2018
3.	System and Unit Testing	June 2, 2018	June 13, 2018
4.	UAT & Deployment	June 16, 2018	July 27, 2018
5.	Go Live	TBD	

Phase and Cost Details

Description	Estimated Hours	Rate/hr.	Total
PM & BA	120	$92.00	$11,040.00
Developer	600	$92.00	$55,200.00
Testing & Deployment	160	$92.00	$14,720.00
Total Hours	**880**	**Total Amount**	**$80,960.00**

Terms and Conditions

- The above estimates are based on the agreed upon requirements determined by consultation between PCC and NH SOS. Any unforeseen extra time required to accomplish any of the above tasks shall be communicated to the client and would require approval for the additional time requested.
- These estimates are based on the needs defined by NH SOS.
- The total cost will be based on the above resource usage.

PCC Approval

Signature _____ Title _____ Date _____

Client Approval

Accept [X] Disapprove [ ]

Signature _____ Title DEPUTY SECRETARY OF STATE Date 6/8/18

Comments _____

Centralised Voter Registration System(CVRS)

Two Factor Authentication(TFA) Release Notes

PCC Technology, Inc.

100 Northfield Drive

Windsor, CT 06095

860-242-3299

www.pcctg.com

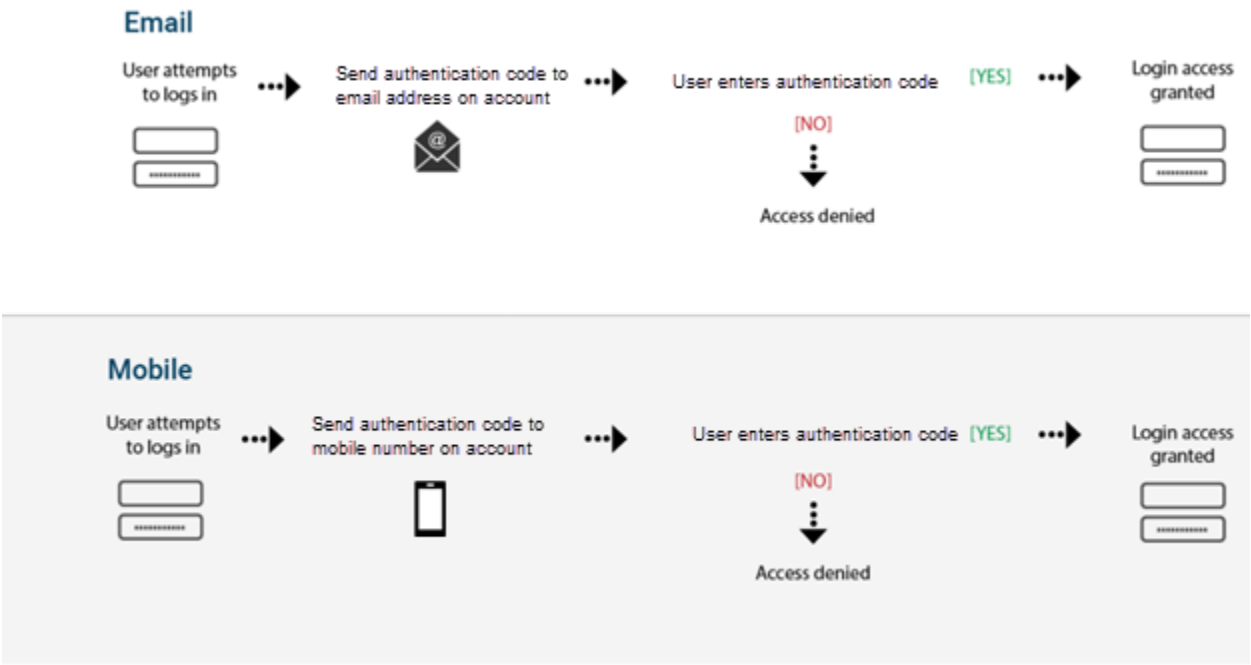
Version History:

Version	Date	Author(s)	Description
1.0	09/25/2018	Anil Prathipati	Initial version

Contents

I. Introduction

The intent of two-factor authentication(TFA) is to provide more assurance of the identity of the individual attempting to login to CVRS. The below diagram shows the two-factor authentication flow that the user will have to go through based on whether the user has selected the option of receive the authentication code via email or mobile device.



The flow begins when the user attempts to log into CVRS by entering the credentials and the system will provide the option to select how the user wishes to receive the authentication code. Based on this there are two outcomes.

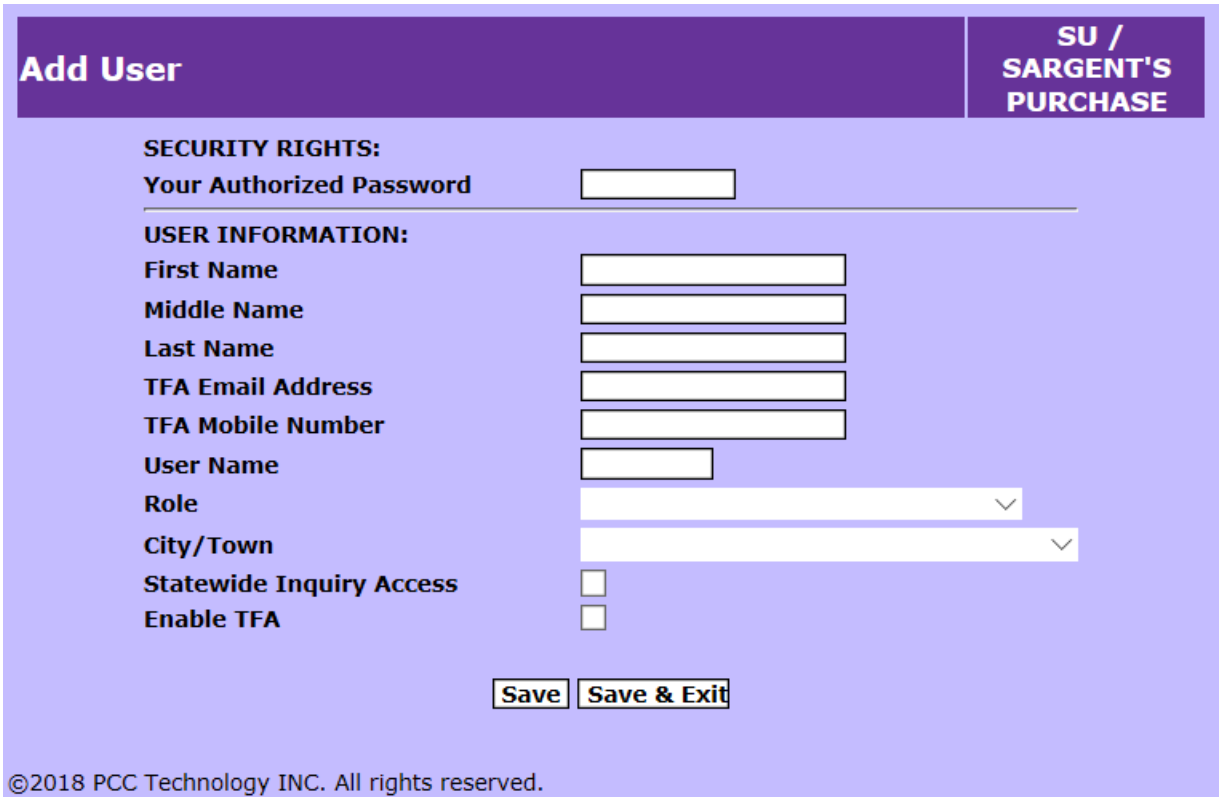
- If the user chooses to receive the code via email, then the authentication code will be sent to the e-mail address on the user account.
- If the user chooses to receive the code to a mobile device, then the authentication code will be sent to the mobile number on the user account.

The user will then enter the authentication code received to login to the CVRS.

The following changes are made to the CVRS application to implement this functionality.

1. User Profile

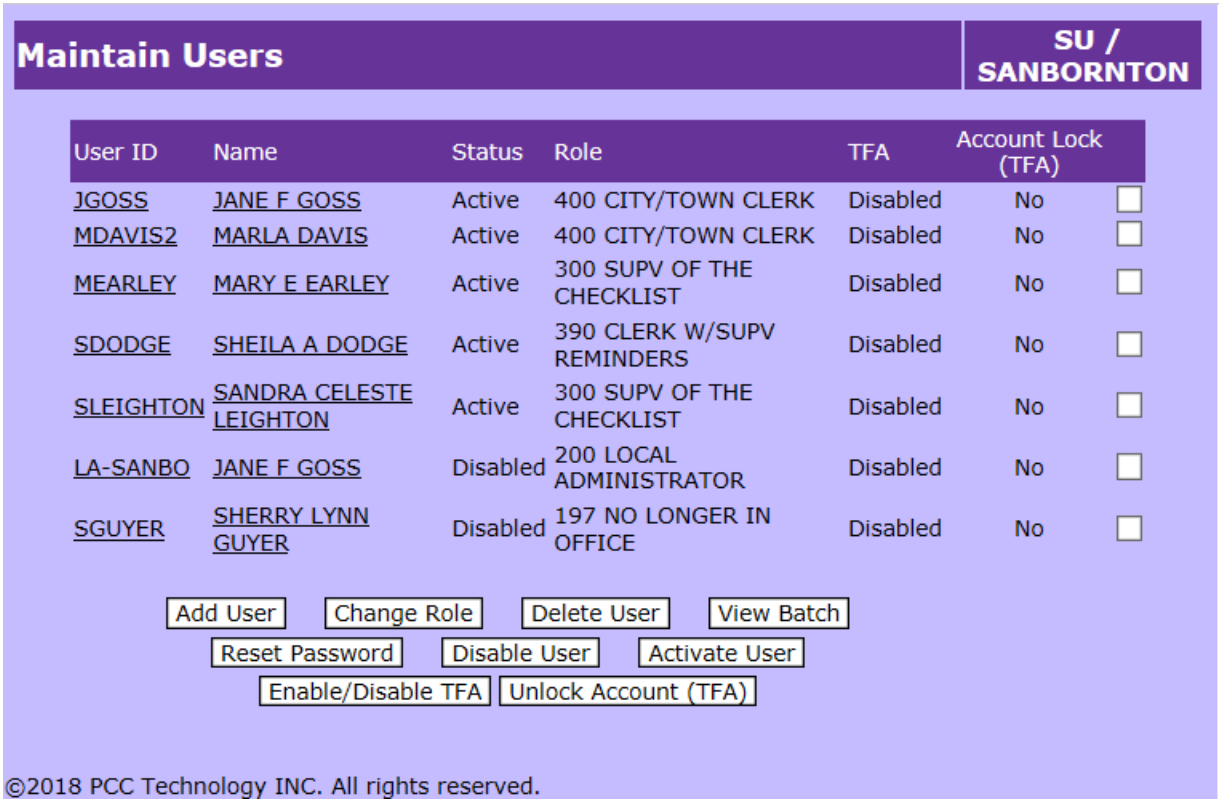
The **System -> Maintain Users** screen is updated to add a new field to allow user to enter the email address and mobile number. When a new user account is created, or an existing user profile is updated by authorized user, provision is made to enter the mobile number and/or email address. One of these are required fields.



The mobile number will be displayed in XXX-XXX-XXXX format.

A new button is added to the user profile that is used to indicate if the user account is locked for generating the authentication code. The button labeled **'Unlock Account (TFA)'** is added to the user profile and if a user account is locked for entering the authentication code incorrectly for a specified number of times then the authorized user can unlock the user account by clicking on the **'Unlock Account (TFA)'**.

1.1 Screen



A new button "**Enable/Disable TFA**" is added to System administrator to control user level two-factor authentication process. System administrator can enable or disable TFA for a user by selecting the check box and click on "**Enable/Disable TFA**" button. The users whose TFA is enabled should go through TFA to login to application if the users County and Role is enabled with two factor authentication.

The system will use the mobile number and e-mail address on the user profile to send the verification link and authentication code.

- For mobile number the system will send the verification link and authentication code to US numbers only.
- **My Information** screen is updated to display the mobile number entered in the **'Maintain Users'** screen.

2. User Login

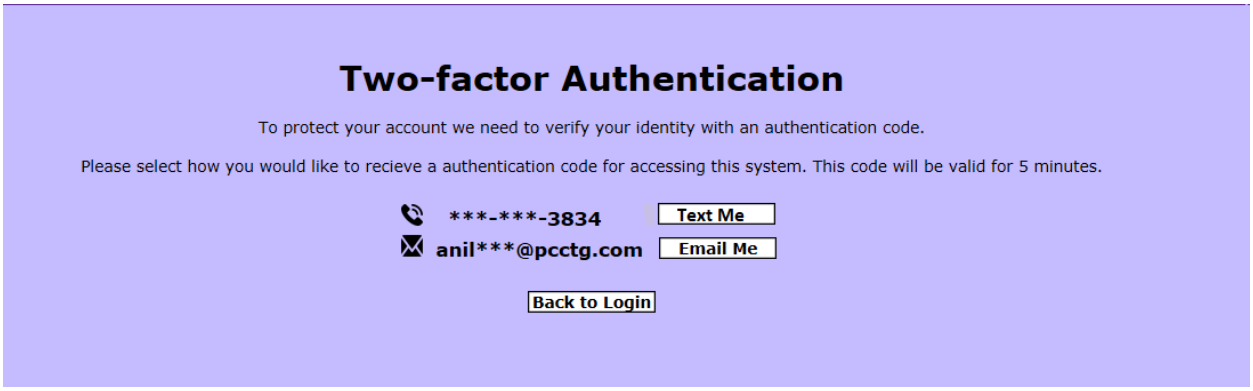
With the implementation of the two-factor authentication functionality all the users logging into CVRS will have to go through following process.

Process

- User enters the credentials and successfully logs in and the system will navigate to a secondary screen if the two-factor authentication is turned on.
- This screen will allow the user to select the way they wish to receive the authentication code – either via email or to a mobile number depending on what is available on the user profile.
- Based on the option selected the system will send the authentication code which the user will have to enter in the next screen.
- If the code is entered correctly the system will navigate to the home page.

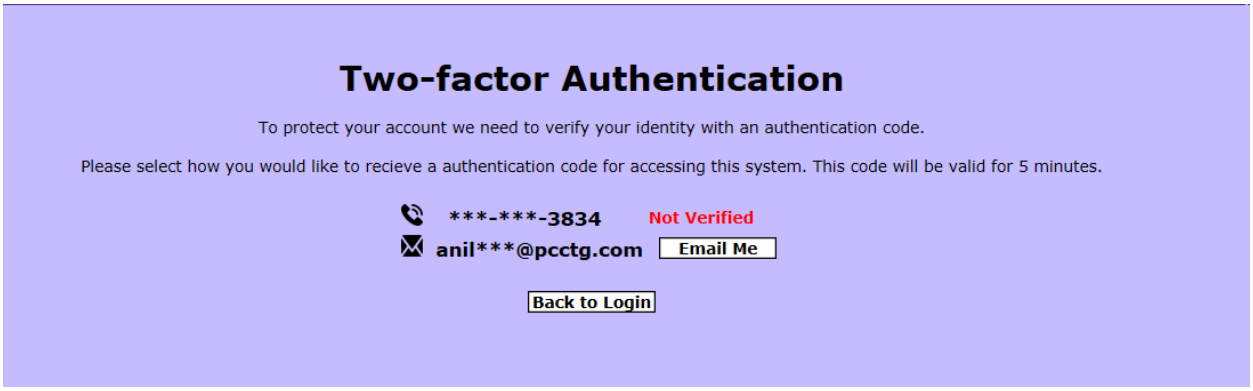
2.1 Screen

Mode To Receive The Authentication Code screen



- If no mobile number or e-mail address is present on the user profile, then the system will display an alert message when the user tries to login to CVRS and the message will say - **The User ID you entered is not associated with an e-mail address or a mobile number. An e-mail address or mobile number must be listed on your profile account to receive an authentication code. If you have a valid username, please contact your State Administrator for further assistance.**
- The system will allow user to select either email or mobile number to receive the authentication code (depending on which is available on the user profile and is verified).
- The system will display mobile number as an option to receive the authentication code if
  - Mobile authentication is turned on by the authorized user.
- The system will display email address as an option to receive the authentication code if
  - Email authentication is turned on by the authorized user.

- If mobile number or email address is available on the user profile but if it is not verified, then the system will display this information with a status **'Not Verified'** next to the field and the user will not be able to select that as an option to receive the authentication code unless the verification process is completed.



- For security reasons the system will not display the complete e-mail address or the mobile number of the user on this screen. The system will
  - Display the last four digits and mask the remaining digits of the mobile number.
    For ex: XXX-XXX-1234
  - Display only the first 4 characters of the email id and mask the remaining portion.
    For ex: abcdXXXXXX@county.com
- On clicking **'Email Me' or 'Text Me'** button the system generates the authentication code and sends it to the mode selected and the system navigates to the **'Enter Authentication Code'** screen.

The verbiage in the Email that has the authentication code will be as follows

Subject Line: CVR System Authentication Code
Message Body:

Dear <Insert First Name> <Insert Last Name>,

You are receiving this email because an authentication request was submitted in the CVR System for "<Insert User ID>". Enter the authentication code that appears below to verify your account.

The authentication code for "<Insert User ID>" is: <Insert Code>

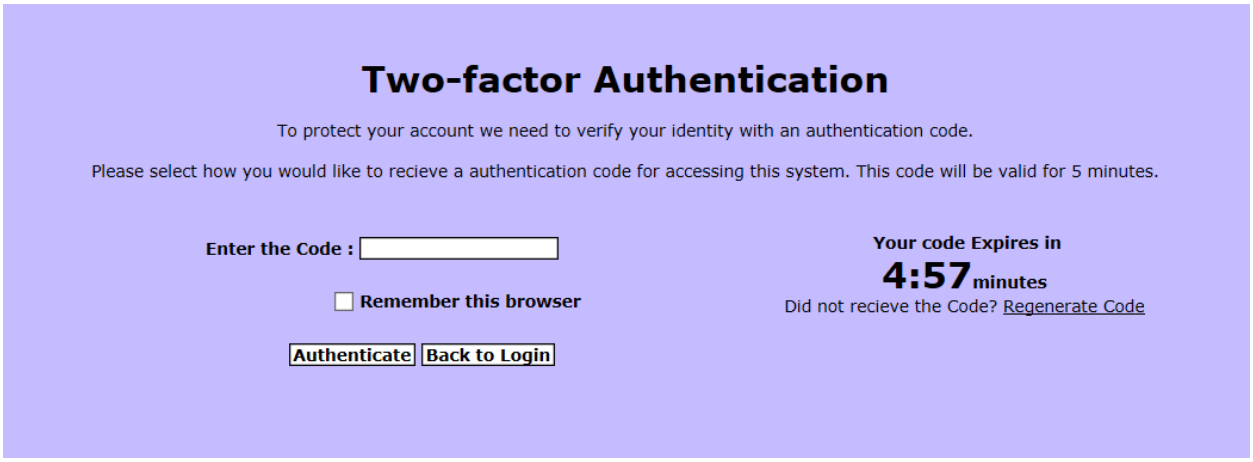
Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

The verbiage in the Text message that has the authentication code will be as follows.
CVRS System Authentication Code for USER ID <Insert User ID> is <Insert Code>.

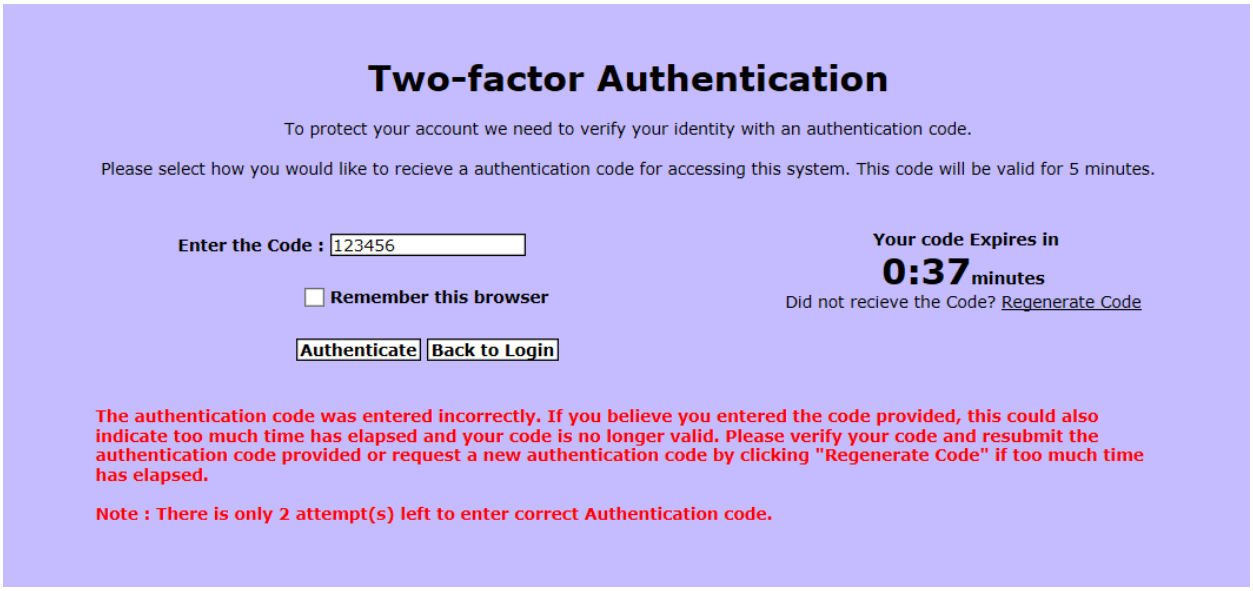
Enter Authentication Code screen

When the authentication code is received the user needs to enter it in the '**TFA Code**' field provided and upon successful authenticating the system will navigate to the home page.



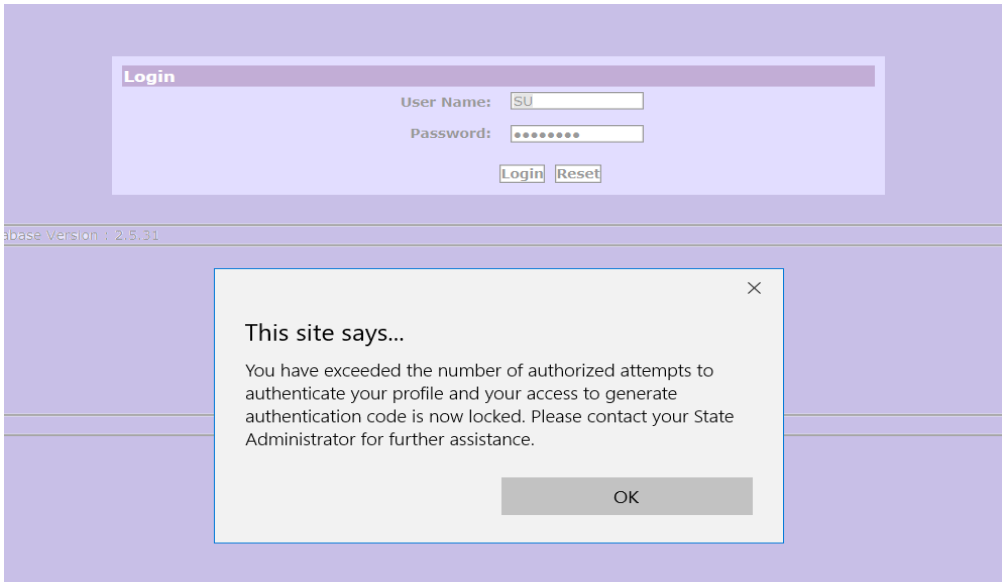
- The authentication code received will always of 6 digits in length.
- If the user wishes to not go through this authentication process again the next time the user tries to log in from the same device(browser), then the user can select **'Remember this browser'** option on this screen. Selecting this checkbox indicates that the browser is trusted, and the user does not have to go through this authentication process until the option is cleared after the number of days set by the authorized user.
- After entering the authentication code correctly, the user needs to click **'Authenticate'** button and the system will navigate to the dashboard screen.
- If for some reason the user does not receive the authentication code, user can request a new code by clicking the **'Regenerate Code'** link. Clicking this link will send a new authentication code to the option previously selected.
- The authentication code received by the user will have a validity that is set by the authorized user after which the code becomes invalid. The system will display a countdown timer on this screen that indicates the length of time the code is valid. Once the code becomes invalid the user cannot use it and the user will have to request a new code by clicking **'Regenerate Code'** link.
- If the user wishes to navigate back to the login screen, then the user can click on **'Back to login '** button. Clicking this button will navigate to the login screen.

If the authentication code was entered incorrectly or if the user enters an expired code and upon clicking **'Authenticate'** button the system will display the following alert message – **The authentication code was entered incorrectly. If you believe you entered the code provided, this could also indicate too much time has elapsed, and your code is no longer valid. Please verify your code and resubmit the authentication code provided or request a new authentication code by clicking "Regenerate Code" if too much time has elapsed**.



When the user enters the code incorrectly and clicks **'Authenticate'** button and there is only one more attempt left before the account is locked the system displays an alert message which says – **Note: There is only one attempt left to enter correct Authentication code.**

If the user enters the authentication code incorrectly for a predefined number of times the system locks the user account's ability to generate the authentication code and logs the user out and displays an alert message - **You have exceeded the number of authorized attempts to authenticate your profile and your access to generate authentication code is now locked. Please contact your State Administrator for further assistance**.

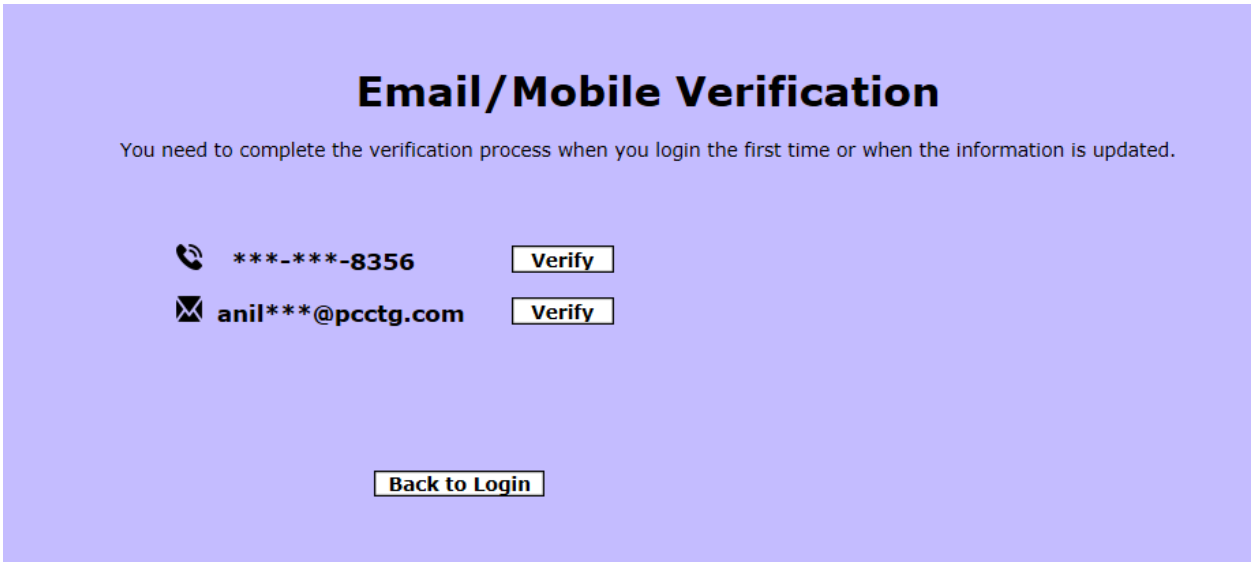


Email Address and Mobile Number Verification

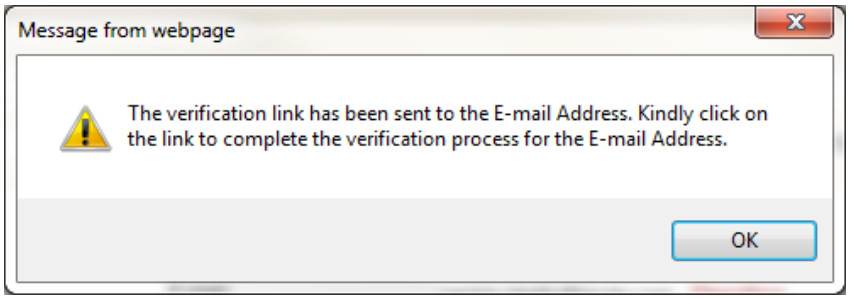
An additional step is included to verify the e-mail address and the mobile number associated with the user profile. This ensures that the e-mail address and/or mobile number entered is correct and that it belongs to the user whose profile is being updated with that information. The user will not be able to continue with the login process unless the e-mail address and/or the mobile number is verified. The verification of e-mail address and mobile number will be a one-time process, unless the e-mail address or mobile number is updated. The following steps must be followed by the users to verify the e-mail address and/or mobile number.

New User

- State User will add the new user with all the required information in CVRS.
- The new user will try to log into CVRS using the credentials shared.
- Upon successfully logging in the system will display an intermediate screen for the user to verify the e-mail address and/or mobile number available on the profile. On this screen the system will display the e-mail address and the mobile number along with a **'Verify'** button next to each of them.



- Clicking the **'Verify'** button next to the e-mail address will send an email which contains a link to the e-mail address being verified. The system will also display a confirmation message saying that the verification link is sent.



The verbiage in the Email that has the verification link will be as follows.
Subject Line: *CVRS E-mail Verification*

Dear <Insert First Name> <Insert Middle Name> <Insert Last Name>,

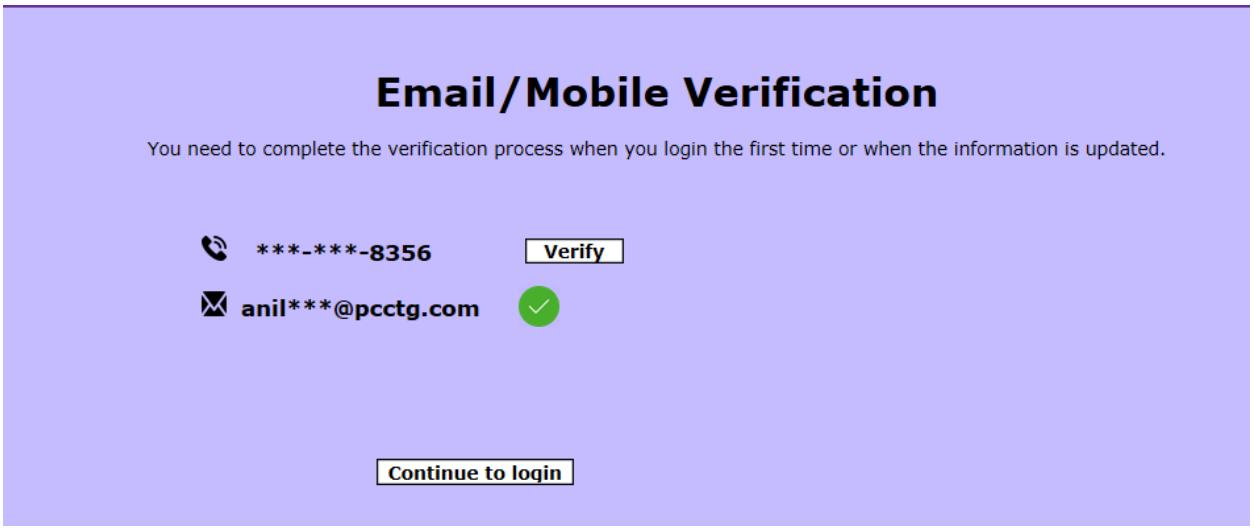
This e-mail address is associated with the USER ID: "<Insert User ID>". Please click on the following link to verify this e-mail address.

The verification of this e-mail address will remain in effect until the e-mail address is changed or the user profile is deleted. Once you verify this e-mail address, you will be able to receive your authentication code using this e-mail address, in order to proceed logging into the CVRS. As a reminder, you will be required to authenticate your web browser periodically after the initial authentication. This e-mail address will be available for use each time you submit a request for an authentication code.

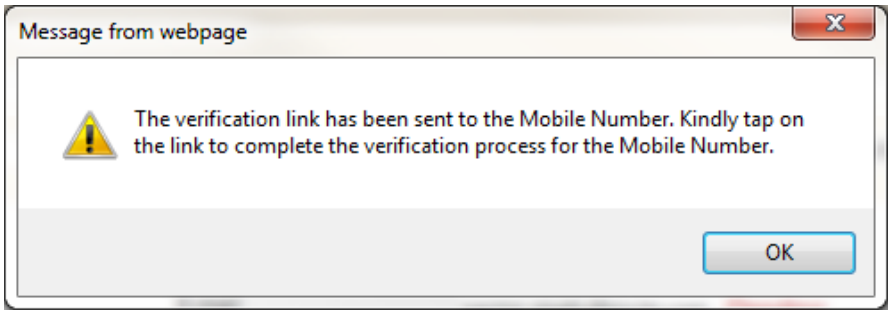
To verify this e-mail address, click here <Insert link>

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

- The user needs to open the email and click the link to complete the verification process and the system will display a confirmation page that says **Email Address is verified**.
- Now if the user comes back to CVRS application the system will be display a status which says  next to the e-mail address on the intermediate screen.



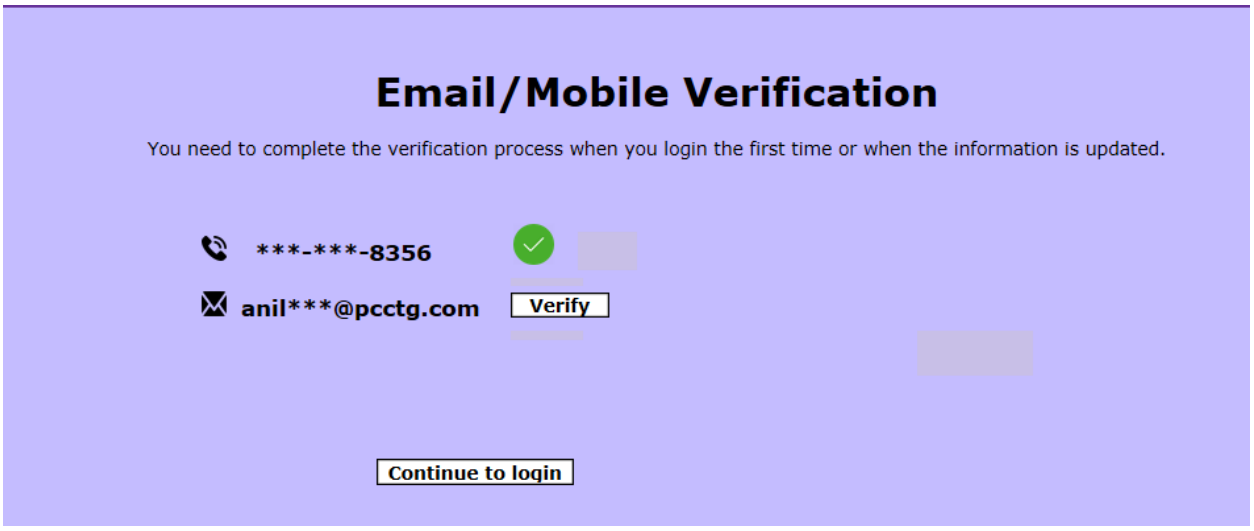
- The user can follow the same steps to verify the mobile number as well. Clicking the '**Verify**' button next to the mobile number will send a text message which contains a link to the mobile number being verified. The system will also display a confirmation message as well.



The verbiage in the Text message that has the verification link will be as follows.
CVRS Verification. Tap below link to verify your phone: XXXXXXXXX.

The user needs to open the text message received and tap the link to complete the process and the mobile number is now verified.

- Now if the user comes back to application the system will be display a status as  next to the mobile number on the intermediate screen.



- Unless either the e-mail address and/or the mobile number is verified the users will not be able to complete the authentication process.
- Once this verification process is completed the user needs to logout and log back in again. This can be done by clicking the **'Continue to Login'** button at the bottom of the screen.
- Upon logging back in the system will navigate to the two-factor authentication screen and the user can complete the login process.
- After logging in the user can view the status of the e-mail address and the mobile number on **My Information** which displays  status next to them.

- And, anytime the user updates the e-mail address or mobile number a button to verify the field will be displayed next to the updated field. The user needs to verify the updated information to continue receiving the authentication code to the new e-mail address or mobile number.

Note:

- Upon updating both the e-mail address and mobile number if the user does not verify these from **My Information** screen then when the user logs in to CVRS the next time the system will ask the user to verify the information before proceeding.
- If the user updates either the e-mail address or the mobile number and does not verify the updated information from **My Information** and when the user logs into CVRS the next time the system will display the updated e-mail address or mobile number to receive the authentication code, but the user will not be able to select it. It will be displayed with a status of **'Not Verified'**. However, the user will still be able to complete the authentication process by receiving the code on the existing verified email address or mobile number.

3. My Remembered Devices

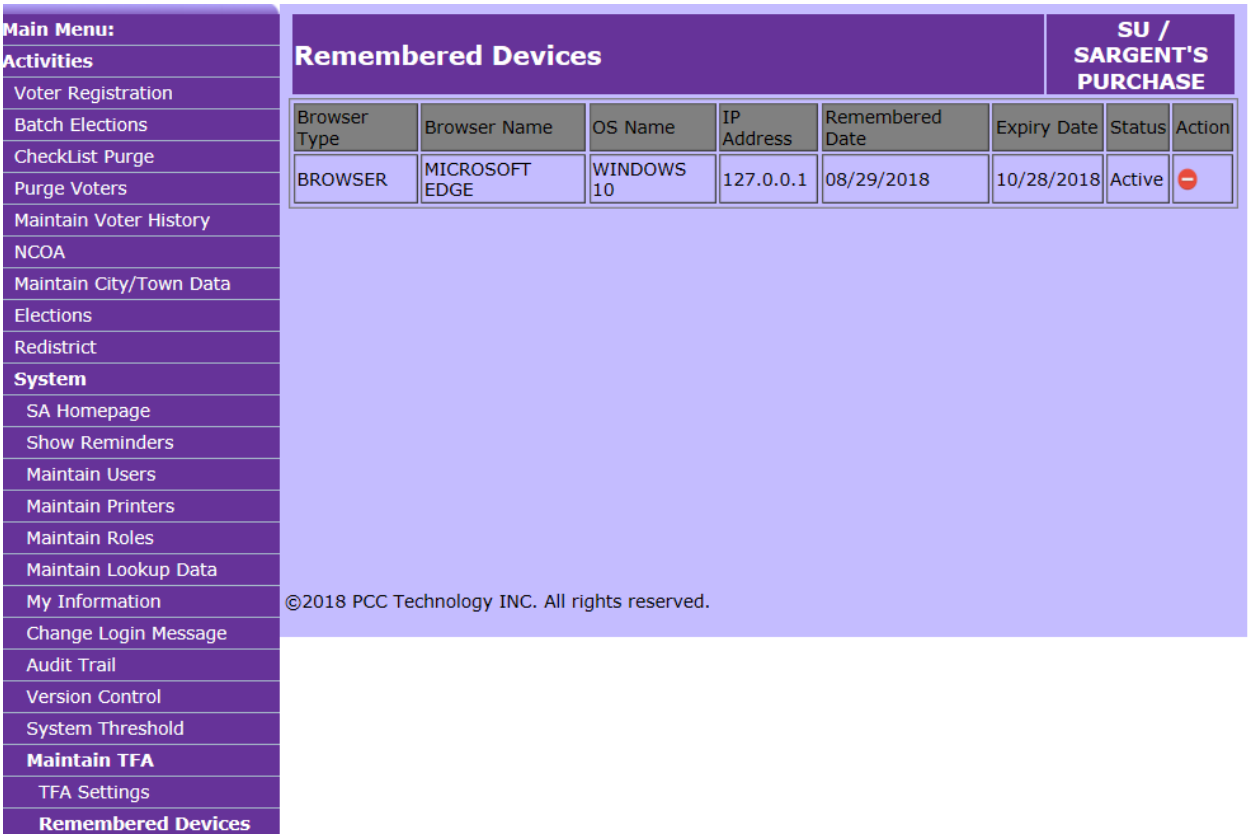
The system also provides the option for the user to view the browsers that have been authenticated (when they select the **'Remember this browser'** option). To view this the user can navigate to **System -> Maintain TFA -> Remembered Devices** screen. This screen will display the details like the Remembered Date, Expire Date, Browser Type, Browser Name, OS Name, IP Address from where they selected **'Remember this browser'** option.

Clicking  icon under the **Actions** column will delete the entry from the list.

Note:

- If the record for the most recent entry for the browser and IP Address combination is deleted, then the user will have to go through the two-factor authentication when the user logs in using that browser from that system.

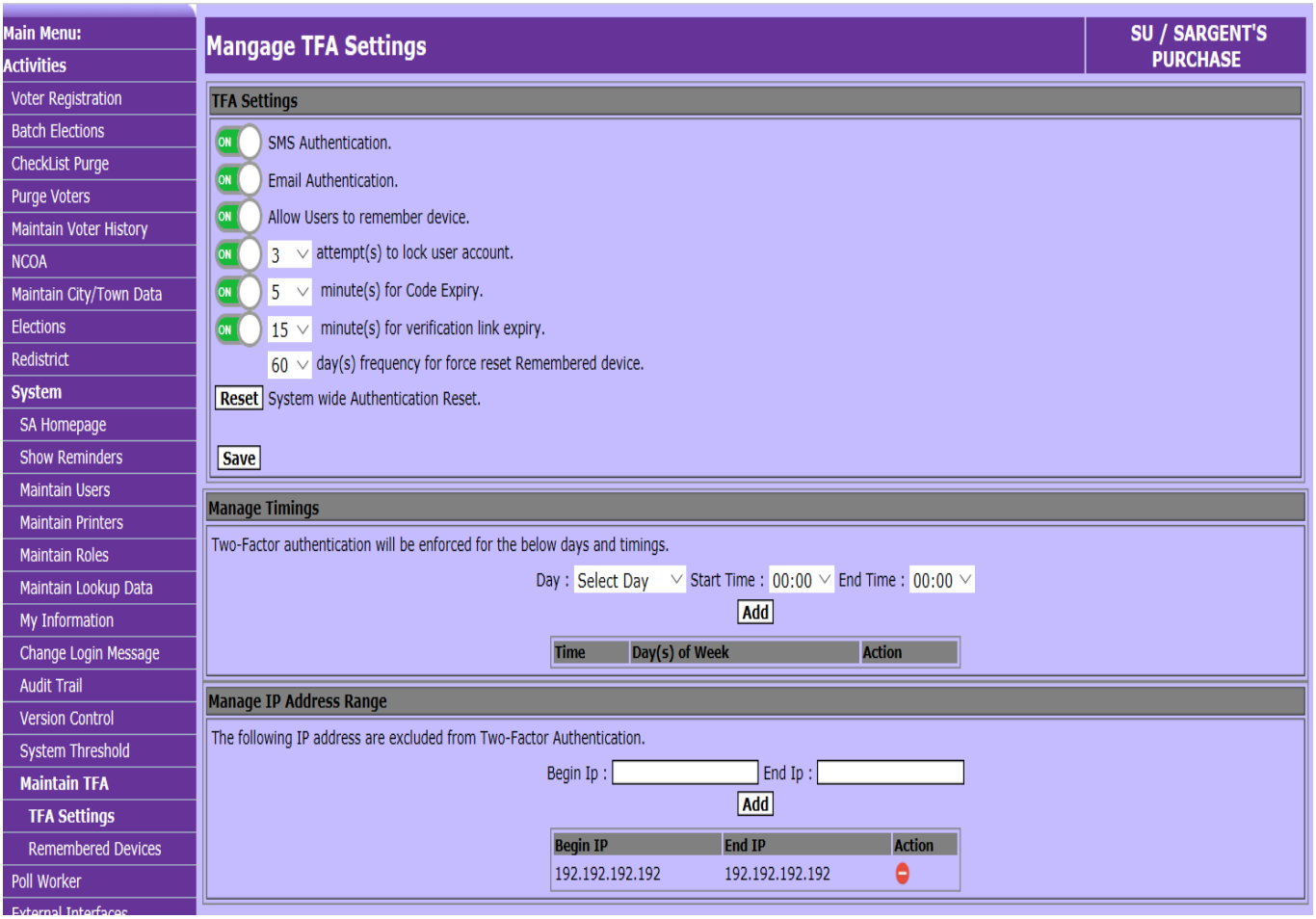
3.1 Screen



4. Two-factor Authentication Settings Management

The system will provide the authorized user with options to manage the various parameters related to the two-factor authentication. This is accomplished by providing a new screen under **System -> Maintain TFA -> TFA Settings** which will list all the configurable fields.

4.1 Screen

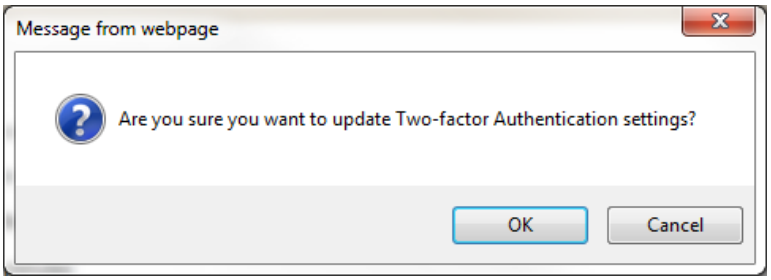


The system will allow the authorized user to turn ON or OFF the various parameters associated with two-factor authentication.

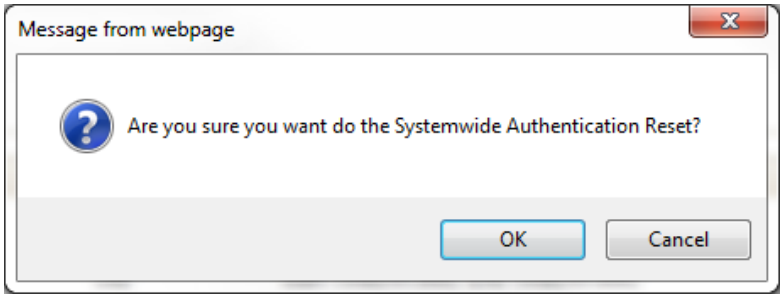
- **Email Authentication** - The system will allow the authorized user to turn ON or OFF the option to receive the authentication code to an e-mail address. Turning this option ON will display the e-mail address if it is available on the user account as an option to receive the authentication code on the **'Mode to receive the authentication code'** during the login process. If this is turned OFF, then the system will not display e-mail address as option to receive the authentication code on the **'Mode to receive the authentication code'** screen.

- **SMS Authentication** - The system will allow the authorized user to turn ON or OFF the option to receive the authentication code to a mobile number. Turning this option ON will display the mobile number if it is available on the user account as an option to receive the authentication code on the **'Mode to receive the authentication code**' during the login process. If this is turned OFF, then the system will not display mobile number as option to receive the authentication code on the **'Mode to receive the authentication code**' screen.
- **Allow users to Remember device -** The system will allow the authorized user to turn ON or OFF the option to allow the users to select the **'Remember this browser'** option. Turning ON this option will display the **'Remember this browser'** option on the **'Enter authentication code'** screen and the user will be able to select it during the authentication process. If this is turned OFF, then the system will not display the **'Remember this browser'** option on the **'Enter authentication code'** screen.
  Note: If this option is turned OFF all the users who have not selected **'Remember this browser'** previously will have to go through the two-factor authentication process every time they login and all the users who have selected **'Remember this browser'** previously will continue to login without the authentication process until the clock is over. Once the clock is over the users will have to go through the two-factor authentication process every time they login.
- **Force Reset Remember this device** - The system will allow the authorized user to reset the '**Remember this browser'** option every **X** number of days.
  Note: If the user changes the number of days for this parameter, the updated days will be applicable only for the users logging in and those who select **'Remember this browser'** after the change is made. All the previous users will continue the old clock and they will have to select the **'Remember this browser'** again upon logging in when the old clock expires.
- **TFA code expires in Minutes** - The system will also provide option for the authorized user to set the validity (in minutes) of the authentication code being sent. By default, 5 minutes will be selected.
- **Verification link expires in Minutes** - The system will also provide option for the authorized user to set the validity (in minutes) of the verification link being sent. By default, 15 minutes will be selected.
- **Lock User Account after failed attempts**- The system will also provide option for the authorized user to set the number of attempts allowed for the incorrect authentication code to be entered before locking the user account.

  After making any of the above changes the user can click
  - **'Save'** button for the changes to take effect. On clicking this button, the system will display an alert message asking if the user wants to continue. The user can click 'OK' to confirm or 'Cancel' to not save the changes.



- **Systemwide Reset** – This is like a master reset that will force all the users to go through the authentication process. Clicking **'Force Reset'** button will force all the users to go through the authentication process irrespective of whether the user selected **'Remember this device'** previously or not. On clicking this button, the system will display an alert message asking if the user wants to continue. The user can click 'Ok' to confirm or 'Cancel' to not save the changes.



- **Manage IP Address** - The authorized user will also be able to manage the **IP Addresses** that will be not be required to go through this two-factor authentication process. The user can enter the Beginning and Ending IP Addresses (in **X.X.X.X** format) that will be excluded from the two-factor authentication process. The IP addresses added will be exempt from two-factor authentication process until they are removed from the list.
  - Click the **'Add'** button and the system adds the IP Address Range to the grid and excludes them from the two-factor authentication process.
  - Click the delete icon under **Actions** column to delete the selected information from the grid.

- **Manage Timings –** The screen will also provide option for the authorized user to set specific times of the days of the week, so that the users logging into CVRS will have to go through the two-factor authentication. If any time of the day is set under **'Manage Timings'** and if any user tries to login to CVRS between these times, then they will have to go through the two-factor authentication process irrespective of whether the user selected **'Remember this browser'** previously.

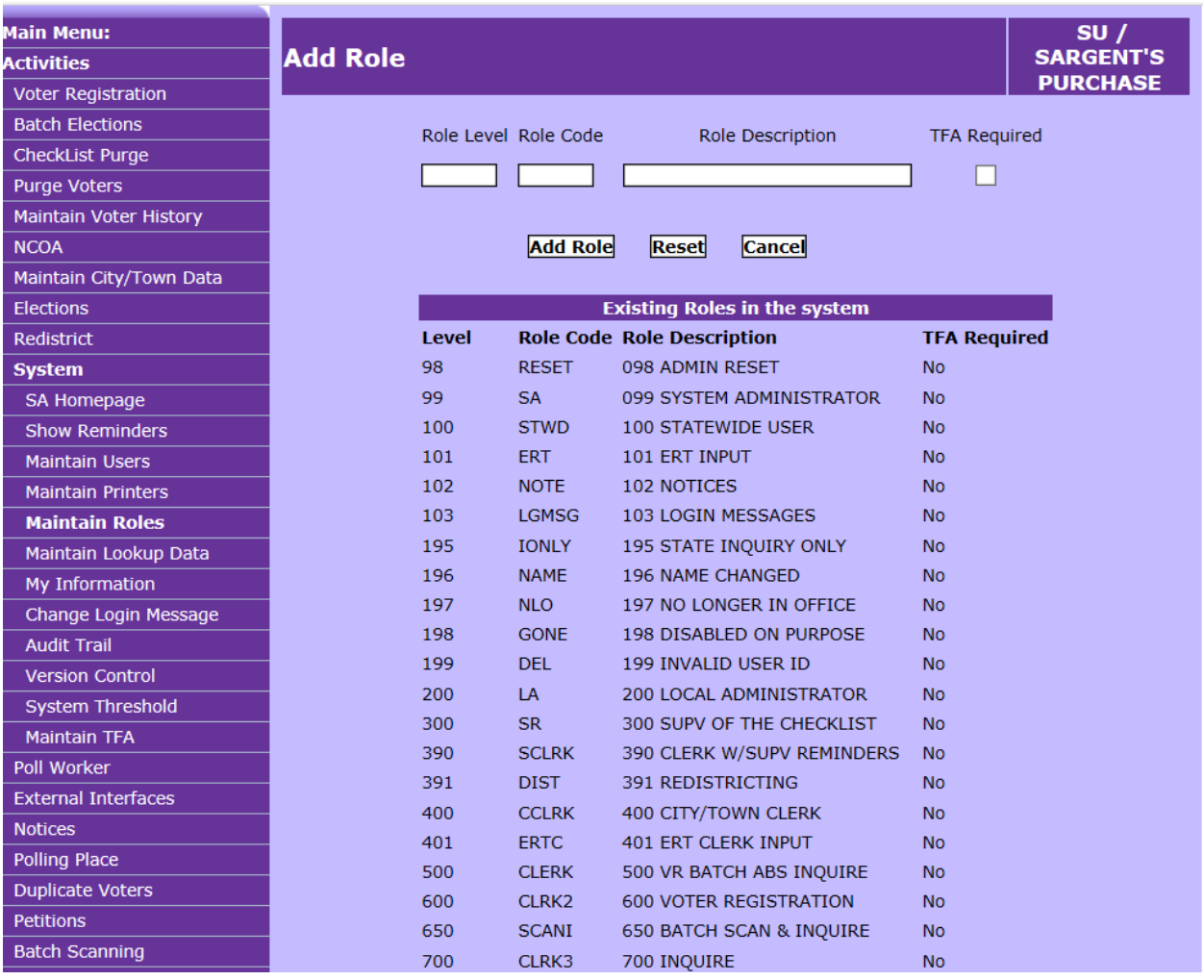
  Note:
  - TFA will not be enforced during these timings for those roles who do not have TFA enabled, for the counties not enabled and those IP Addresses that are whitelisted.

- For TFA to be enforced during these timings **Email Authentication** and **SMS Authentication** needs to be turned ON.
- **'Remember this browser'** option will not be enabled during these timings.

5. Maintain Roles

When the new roles are created, or the existing roles are updated the system will allow authorized user to select which user roles will have to go through the two-factor authentication process. The **System -> Maintain Roles** screen is updated by adding a checkbox labeled **'TFA Required'** and the user can select this to indicate if two-factor authentication should be enabled for that role or uncheck it to disable the TFA for that role.

5.1 Screen



- If the checkbox is selected, then then all the users with that role will be required to go through the two-factor authentication process.

Daniel J Cloutier

From: Colleen McCormack on behalf of NHVotes
Sent: Friday, June 14, 2019 4:45 PM
To: NHVotes
Subject: ElectioNet - Two Factor Authentication
Attachments: Password Update 2019-06-11.pdf; 2FA - Two Factor Authentication ElectioNet v5.pdf

Monday, June 17th
Two Factor Authentication & Password Update
will be in Electio*Net* Live and Playground

- Security Updates will go into effect on Monday, June 17th
- 2FA – Two Factor Authentication
  - If you have provided us with at least one method of verification on your RAE form, you may proceed with the Two Factor Authentication.
  - The full instructions for 2FA are attached.
    - Please follow the instructions to ensure you have verified at least one method.
  - By checking the box "Remember this computer," you will not need to ask for a 6 digit code every time you log in during that day on that computer.
  - After you have completed the log-in process, follow the 2FA instructions to verify the second method that enables you to receive your 6 digit code.
- Password Update
  - You will log in with your current password and then be prompted to change your password after you have completed your Two Factor Authentication.
  - Your password must be updated to be 24 – 50 characters long.
  - The 24 character minimum can be a pass phrase or a combination of 4 or more words.
    - This will be easy to remember if you can visualize your phrase or words.
      - See the examples attached. You will not be able to use any of the examples "exactly" as they are worded for your password.
    - Upper and lower case letters, numeric, special characters and spaces are allowed.
  - Your password will not expire for 6 months.
- If you have any questions or need assistance call the Electio*Net* Help Desk 271-8241.

Thank You,
Elections

Secretary of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, May 30, 2019 12:18 PM
To: Anthony Stevens
Subject: Accepted: 2 Factor Authentication & Virtual Private Network for ElectioNet

Daniel J Cloutier

Subject:	2 Factor Authentication & Virtual Private Network for ElectioNet
Location:	Elections Conference Room at Archives
Start:	Mon 6/3/2019 1:00 PM
End:	Mon 6/3/2019 3:00 PM
Recurrence:	(none)
Meeting Status:	Accepted
Organizer:	Anthony Stevens
Required Attendees:	Daniel J Cloutier; David Scanlan; Colleen McCormack; Orville Fitch; Adrian S. LaRochelle

Meeting with Sec. Gardner to go over strategy to proceed on two-factor authentication and possibly a virtual private network for the statewide voter registration system.

Meeting on above topic should only take one hour. Starting at 2 PM, meeting will continue with Bill, Dave, Colleen, Bud, and Anthony on elections-related training plans.

Dave, please confirm for Bill – if he can make it.

Daniel J Cloutier

From: Colleen McCormack
Sent: Wednesday, May 29, 2019 3:20 PM
To: NHVotes
Cc: Daniel J Cloutier
Subject: Request for Access Form - RAE
Attachments: Request for Access to ElectioNet 2019-03-07.pdf

To all,
In the near future, we are going to "Two Factor Authentication" (2FA) in the statewide voter registration system (Electio*Net*).

You will log on with your password and then be directed to verify your email address and/or cell phone number. The two-step process will give you an access code to log into Electio*Net*.

I have attached a "Request for Access" (RAE) form for you to complete and return to the Electio*Net* Office. Your address on the form should be the address of your office.
Please return the form by email or fax as soon as possible to: nhvotes@sos.nh.gov or 271-8242.

As we get closer to the roll out of the 2FA, I will send out instructions.

If you have any questions you may call or email me.

Thank You,

Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Tuesday, May 14, 2019 12:26 PM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS. Enter the authentication code that appears below to verify your account.

The authentication code is: 689094.

Do not forward or give this code to anyone. If you did not initiate an authentication request, contact the ElectioNet help desk to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Tuesday, May 14, 2019 12:23 PM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS. Enter the authentication code that appears below to verify your account.

The authentication code is: 938556.

Do not forward or give this code to anyone. If you did not initiate an authentication request, contact the ElectioNet help desk to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Tuesday, May 14, 2019 12:15 PM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS. Enter the authentication code that appears below to verify your account.

The authentication code is: 135032.

Do not forward or give this code to anyone. If you did not initiate an authentication request, contact the ElectioNet help desk to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 3:23 PM
To: Daniel J Cloutier; Colleen McCormack
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: ElectioNet Email functionality

Thank You Dan. It is working now in UAT.

Colleen,
UAT is now using SMTP to send emails. Can you test with your credentials and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 2:58 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: ElectioNet Email functionality

In anticipation of this answer, I entered these two already.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 2:56 PM
To: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: ElectioNet Email functionality

Colleen,

I have already responded to this email. Incase if it is missed following are the details. Thank You.

UAT Server: 10.144.27.27(Application server)
Prod Server: 10.144.27.24(Application server)

Let me know if you need more information. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Friday, April 26, 2019 2:53 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: ElectioNet Email functionality

Bhanu,
Dan will be out all next week. If you could give him an answer today, we possibly test this while he is away.

Thank You,
Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 2:40 PM
To: Bhanu Pothugunta
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Bhanu,

Which actual server is going to initial the SMTP connection?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 2:58 PM
To: 'Bhanu Pothugunta'; Colleen McCormack
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: ElectioNet Email functionality

In anticipation of this answer, I entered these two already.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 2:56 PM
To: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: ElectioNet Email functionality

Colleen,

I have already responded to this email. Incase if it is missed following are the details. Thank You.

UAT Server: 10.144.27.27(Application server)
Prod Server: 10.144.27.24(Application server)

Let me know if you need more information. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Friday, April 26, 2019 2:53 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: ElectioNet Email functionality

Bhanu,

Dan will be out all next week. If you could give him an answer today, we possibly test this while he is away.

Thank You,

Colleen

Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 2:40 PM
To: Bhanu Pothugunta
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Bhanu,

Which actual server is going to initial the SMTP connection?

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 2:43 PM
To: Daniel J Cloutier
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Dan,

Here are the details:

UAT Server: 10.144.27.27(Application server)
Prod Server: 10.144.27.24(Application server)

Let me know if you need more information. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 2:40 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Bhanu,

Which actual server is going to initial the SMTP connection?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 2:56 PM
To: Colleen McCormack; Daniel J Cloutier
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: ElectioNet Email functionality

Colleen,

I have already responded to this email. Incase if it is missed following are the details. Thank You.

UAT Server: 10.144.27.27(Application server)
Prod Server: 10.144.27.24(Application server)

Let me know if you need more information. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Friday, April 26, 2019 2:53 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: ElectioNet Email functionality

Bhanu,
Dan will be out all next week. If you could give him an answer today, we possibly test this while he is away.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 2:40 PM
To: Bhanu Pothugunta
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Bhanu,

Which actual server is going to initial the SMTP connection?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Colleen McCormack
Sent: Friday, April 26, 2019 2:53 PM
To: Daniel J Cloutier; Bhanu Pothugunta
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: ElectioNet Email functionality

Bhanu,
Dan will be out all next week. If you could give him an answer today, we possibly test this while he is away.

Thank You,
Colleen
Colleen E. McCormack
Secretary of State - Elections
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
ElectioNet Help Desk Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 2:40 PM
To: Bhanu Pothugunta
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Bhanu,

Which actual server is going to initial the SMTP connection?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:

2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 2:40 PM
To: 'Bhanu Pothugunta'
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Bhanu,

Which actual server is going to initial the SMTP connection?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Friday, April 26, 2019 12:39 PM
To: Daniel J Cloutier
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

Thank You Dan.

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Friday, April 26, 2019 12:38 PM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:

2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Friday, April 26, 2019 12:38 PM
To: 'Bhanu Pothugunta'
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: RE: Electionet Email functionality

There is no username and password for that shared mailbox. If it didn't work, it may because we were having trouble with our outbound email connector or NHVotes is not yet in the allow to relay bucket. I am checking the bucket and will let you know what I find.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Thursday, April 25, 2019 5:03 PM
To: Daniel J Cloutier
Cc: Keval Patel; Colleen McCormack; Anil Kumar Prathipati
Subject: Electionet Email functionality

Dan,

We are working on the SMTP email configuration in UAT. We could able to send emails to state network email addresses(SOS.NH.GOV) without user name and password but failing to send emails to outside domain.
Can you share username and password for NHVotes@sos.nh.gov. We will test and see if it works with username and password.

Following is the error we are receiving:
javax.mail.SendFailedException: Invalid Addresses;
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) nested exception is:
2019-04-25 16:36:25,023 ERROR [stderr] (default task-1) com.sun.mail.smtp.SMTPAddressFailedException: 550 5.7.54 SMTP; Unable to relay recipient in non-accepted domain

Let us know if you have any questions. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Wednesday, April 17, 2019 11:39 AM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID HD-DCLOUT. Enter the authentication code that appears below to verify your account.

The authentication code for USER ID HD-DCLOUT is: 840388.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Wednesday, April 17, 2019 12:14 PM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID HD-DCLOUT. Enter the authentication code that appears below to verify your account.

The authentication code for USER ID HD-DCLOUT is: 760007.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Wednesday, April 17, 2019 11:58 AM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID HD-DCLOUT. Enter the authentication code that appears below to verify your account.

The authentication code for USER ID HD-DCLOUT is: 368396.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Wednesday, April 17, 2019 11:34 AM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID HD-DCLOUT. Enter the authentication code that appears below to verify your account.

The authentication code for USER ID HD-DCLOUT is: 886450.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: Gerow, Donald <Donald.Gerow@doit.nh.gov>
Sent: Tuesday, March 19, 2019 9:20 AM
To: Scott C. Caveney
Cc: Colleen McCormack; Daniel J Cloutier; White, Brenton
Subject: RE: NHVotes email verification - Spoofed

Scott,

Thanks, we will let them be delivered.

Amazon sending emails out with the **NHVotes@sos.nh.gov** address is causing the @SOS.NH.GOV domain to be used for DNS Lookup, Reverse Lookup, SPF Record Lookup.

Don

Donald Gerow
GroupWare Applications Management
NH Department of Information Technology
(603) 223-5762

From: Scott C. Caveney <Scott.Caveney@sos.nh.gov>
Sent: Tuesday, March 19, 2019 9:11 AM
To: Gerow, Donald <Donald.Gerow@doit.nh.gov>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Dan Cloutier <daniel.cloutier@sos.nh.gov>
Subject: RE: NHVotes email verification - Spoofed
Importance: High

Don, this is a valid email and not spoofed. I spoke with the Hava Training group which is doing training today and this email was sent by Nicholas Chung Yen. Amazon sends the emails out for NHVotes as I understand it. His account would be NChongyen……

Thanks,

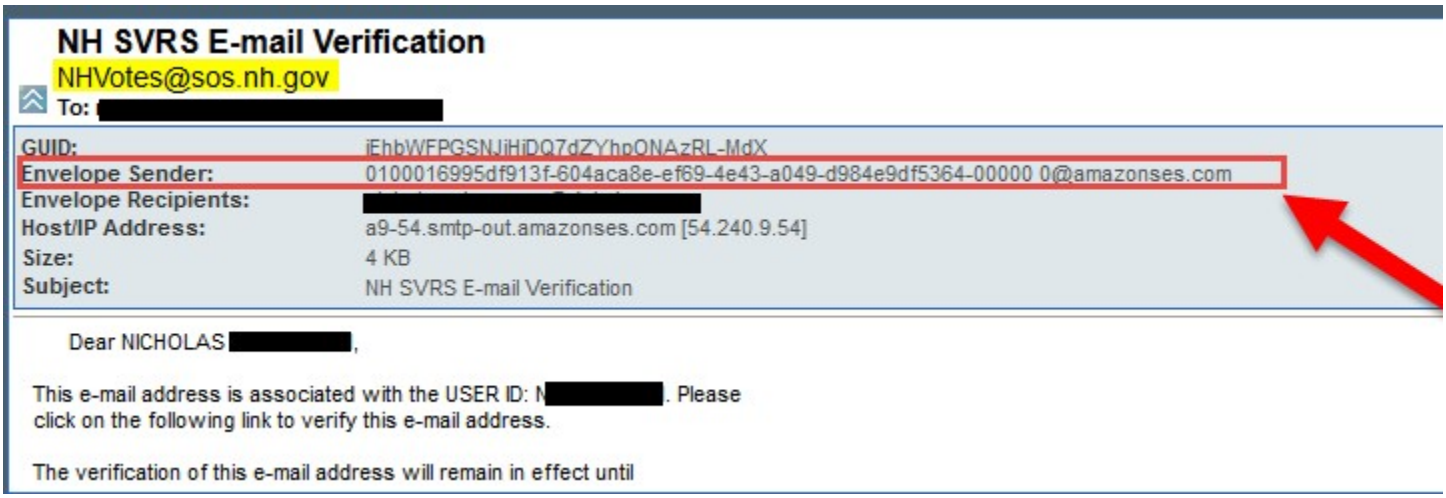
Scott

From: Gerow, Donald [mailto:Donald.Gerow@doit.nh.gov]
Sent: Tuesday, March 19, 2019 8:57 AM
To: Scott C. Caveney
Subject: NHVotes email verification - Spoofed

Scott,

We wanted to checked on some emails that are showing up in our Spoofed email. We got two emails for the same person within 1 second.

The email is showing NHVotes@sos.nh.gov as the sender with a subject of **NH SVRS E-mail Verification**. Showing email coming from @amazonses.com .



Is this something that is going on?

Thank you,
Don

Donald Gerow
GroupWare Applications Management
NH Department of Information Technology
(603) 223-5762

Daniel J Cloutier

From: Scott C. Caveney
Sent: Tuesday, March 19, 2019 9:11 AM
To: 'Gerow, Donald'
Cc: Colleen McCormack; Daniel J Cloutier
Subject: RE: NHVotes email verification - Spoofed

Importance: High

Don, this is a valid email and not spoofed. I spoke with the Hava Training group which is doing training today and this email was sent by Nicholas Chung Yen. Amazon sends the emails out for NHVotes as I understand it. His account would be NChongyen……

Thanks,

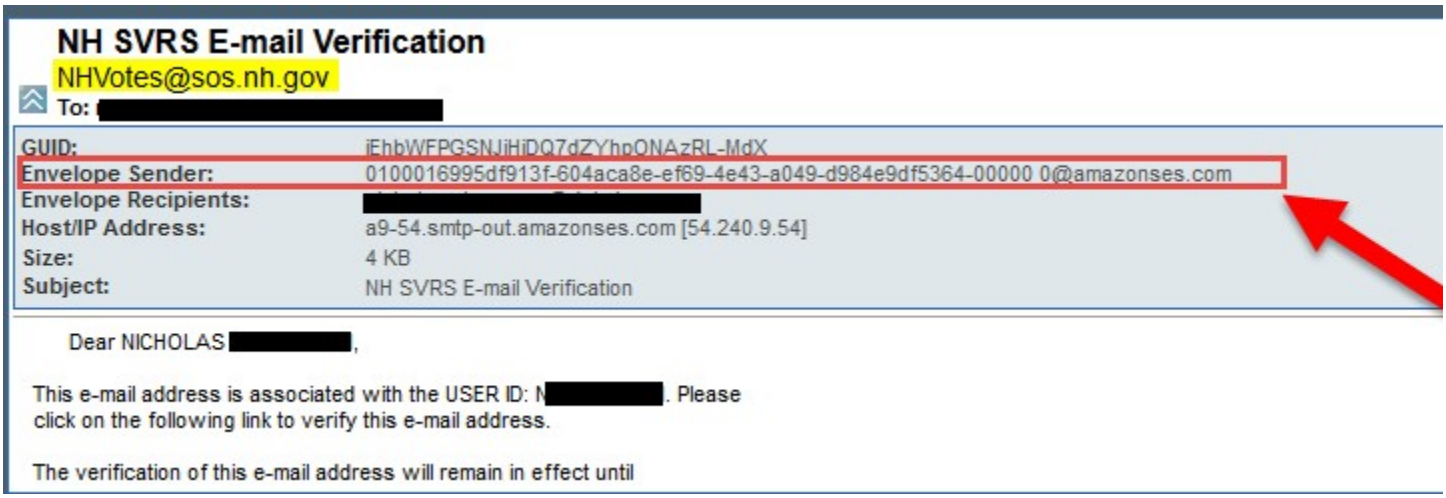
Scott

From: Gerow, Donald [mailto:Donald.Gerow@doit.nh.gov]
Sent: Tuesday, March 19, 2019 8:57 AM
To: Scott C. Caveney
Subject: NHVotes email verification - Spoofed

Scott,

We wanted to checked on some emails that are showing up in our Spoofed email. We got two emails for the same person within 1 second.

The email is showing **NHVotes@sos.nh.gov** as the sender with a subject of **NH SVRS E-mail Verification**. Showing email coming from @amazonses.com .



Is this something that is going on?

Thank you,
Don

Donald Gerow
GroupWare Applications Management
NH Department of Information Technology
(603) 223-5762

Daniel J Cloutier

From: Scott C. Caveney
Sent: Tuesday, March 19, 2019 8:58 AM
To: 'Gerow, Donald'
Cc: Daniel J Cloutier
Subject: RE: NHVotes email verification - Spoofed

Importance: High

Hi Don,

I will have Dan Cloutier look at it from the NHVotes side.

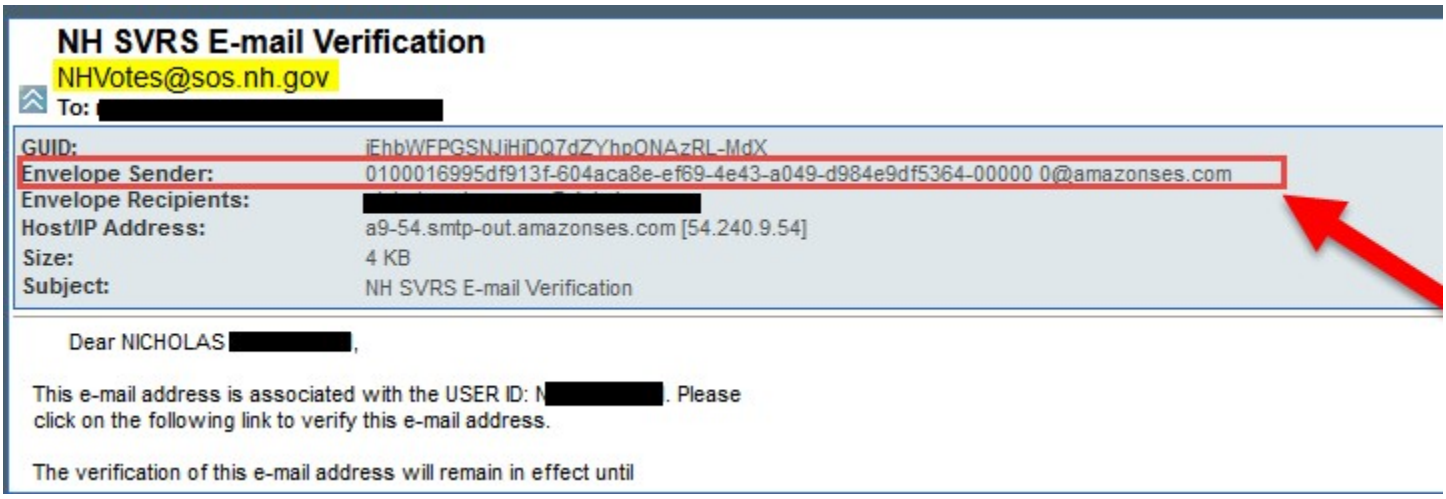
Thanks. Scott

From: Gerow, Donald [mailto:Donald.Gerow@doit.nh.gov]
Sent: Tuesday, March 19, 2019 8:57 AM
To: Scott C. Caveney
Subject: NHVotes email verification - Spoofed

Scott,

We wanted to checked on some emails that are showing up in our Spoofed email. We got two emails for the same person within 1 second.

The email is showing **NHVotes@sos.nh.gov** as the sender with a subject of **NH SVRS E-mail Verification**. Showing email coming from @amazonses.com .



Is this something that is going on?

Thank you,

Don

Donald Gerow
GroupWare Applications Management
NH Department of Information Technology
(603) 223-5762

Daniel J Cloutier

From: Jeffrey King
Sent: Friday, March 1, 2019 10:29 AM
To: Daniel J Cloutier
Subject: RE: ENET training and TFA code

Dan,

I made the updates we talked about yesterday. When searching for a user, you can enter any partial spelling:

To find all cloutier for example, you can enter CLOU and it will return:

Id_User
DCLOUTIER
HD-DCLOUT
JCLOUTIER
MCLOUTIER
NCLOUTIER

Jeff King
Database Administrator
NH Department of State
Jeffrey.King@sos.nh.gov
(603) 271-8823

From: Jeffrey King
Sent: Thursday, February 28, 2019 1:20 PM
To: Daniel J Cloutier
Subject: ENET training and TFA code

Dan,

Take a look at:

Z:\ElectioNet\ENET User Info.accdb

And let me know if this is close to what you think might be needed for training to find the two-factor code.

Jeff King
Database Administrator
NH Department of State
Jeffrey.King@sos.nh.gov
(603) 271-8823

Daniel J Cloutier

From: Jeffrey King
Sent: Thursday, February 28, 2019 1:20 PM
To: Daniel J Cloutier
Subject: ENET training and TFA code

Dan,

Take a look at:

Z:\ElectioNet\ENET User Info.accdb

And let me know if this is close to what you think might be needed for training to find the two-factor code.

Jeff King
Database Administrator
NH Department of State
Jeffrey.King@sos.nh.gov
(603) 271-8823

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, January 31, 2019 12:32 PM
To: Anthony Stevens
Cc: Colleen McCormack
Subject: ElectioNet 2FA

Anthony,

It has come to my attention that the security surrounding ElectioNet 2FA is not as robust as it could/should be. When a user is sent a 2FA code for which they do not act upon that within the specified timeframe, they are left on the same authenticated screen and are able to simply request a new code be sent. Without returning the user to enter their username and password again to retrieve another code, this opens the door for a nefarious individual to bypass that authentication process and potential gain access to ElectioNet data.

My recommendation is to enact the process to return a user to the logon screen if they do not enter the authentication code within the specified timeframe. This will force both the actual user and perhaps a nefarious infiltrator to need access to 2FA in order to authenticate. Without that process, we are back to a single factor authentication.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

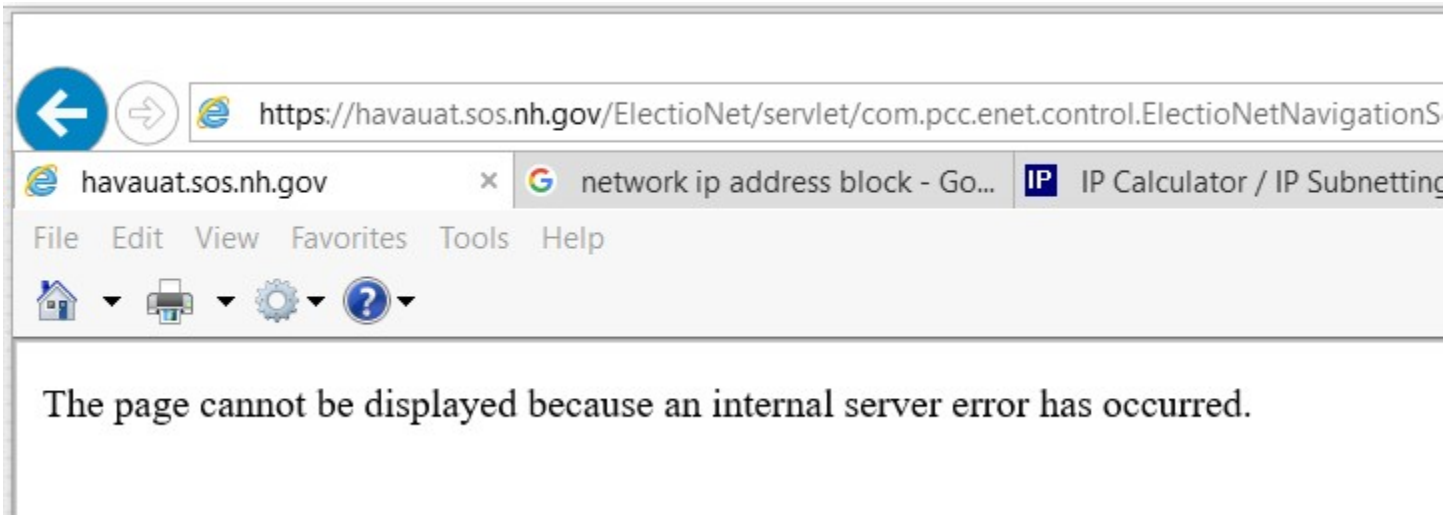
Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

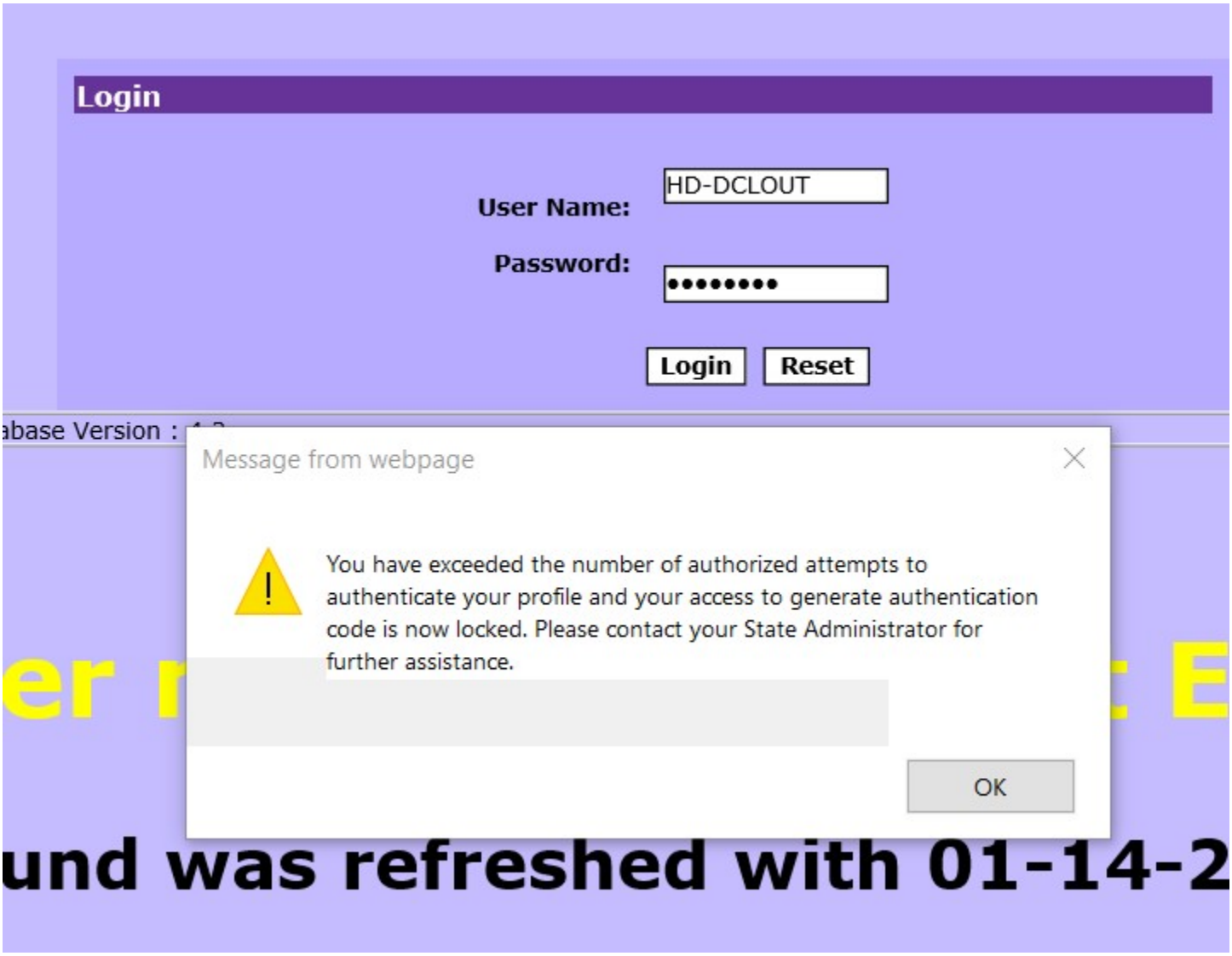
Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, January 31, 2019 11:45 AM
To: Colleen McCormack
Cc: Anthony Stevens
Subject: ElectioNet 2FA

Colleen,

When I had the team on the phone working on getting ProofPoint to allow the 2FA codes to come in without holding them back, I encountered some problems with ElectioNetUAT. Here are the images … feel free to discuss with me:





Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, January 31, 2019 9:34 AM
To: 'Keval Patel'
Cc: Anthony Stevens; Colleen McCormack; Bhanu Pothugunta; Anil Kumar Prathipati; Ganesh Veerabathiran
Subject: RE: Using Amazon for 2-factor authentication

The question is coming up because we have ProofPoint and it has been quarantine the messages. We have found a way to allow the messages through so nothing has to change at this time.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Thursday, January 31, 2019 8:58 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>
Subject: RE: Using Amazon for 2-factor authentication

Amazon service we use for email and SMS both. My experienced with other states AWS response time is very reliable. We can use SOS email server if you have any concerns but we still need to use AWS service for SMS. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, January 31, 2019 8:37 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Using Amazon for 2-factor authentication

Keval,

Why are we using an Amazon service to send the 2FA messages instead of using our own SOS email server?

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Thursday, January 31, 2019 8:58 AM
To: Daniel J Cloutier
Cc: Anthony Stevens; Colleen McCormack; Bhanu Pothugunta; Anil Kumar Prathipati; Ganesh Veerabathiran
Subject: RE: Using Amazon for 2-factor authentication

Amazon service we use for email and SMS both. My experienced with other states AWS response time is very reliable. We can use SOS email server if you have any concerns but we still need to use AWS service for SMS. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, January 31, 2019 8:37 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Using Amazon for 2-factor authentication

Keval,

Why are we using an Amazon service to send the 2FA messages instead of using our own SOS email server?

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, January 31, 2019 8:37 AM
To: 'Keval Patel'
Cc: Anthony Stevens; Colleen McCormack
Subject: Using Amazon for 2-factor authentication

Tracking:

Recipient	Read
'Keval Patel'	
Anthony Stevens	Read: 1/31/2019 9:05 AM
Colleen McCormack	

Keval,

Why are we using an Amazon service to send the 2FA messages instead of using our own SOS email server?

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, January 22, 2019 10:48 AM
To: 'Bhanu Pothugunta'; Colleen McCormack
Subject: RE: ElectioNet UAT - 2FA Issue

I was just able to successfully authenticate using my uat test account.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Tuesday, January 22, 2019 10:42 AM
To: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

AWSProxy site was down for a while due to some firewall issue. Our IT administrator is looking into it. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 10:31 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: ElectioNet UAT - 2FA Issue

It is now working. What happened?

Thank You,
Colleen
Colleen E. McCormack
HAVA

Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, January 22, 2019 10:26 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

It is working now. Can you please test and let me know if you are still having issues. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up "00 – Error occurred."
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word "Occured". It should be spelled "Occurred" (2 r's)

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Tuesday, January 22, 2019 10:47 AM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID HD-DCLOUT. Enter the authentication code that appears below to verify your account.

The authentication code for USER ID HD-DCLOUT is: 104750.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Tuesday, January 22, 2019 10:42 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

AWSProxy site was down for a while due to some firewall issue. Our IT administrator is looking into it. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 10:31 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: ElectioNet UAT - 2FA Issue

It is now working. What happened?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, January 22, 2019 10:26 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

It is working now. Can you please test and let me know if you are still having issues. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up "00 – Error occurred."
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word "Occured". It should be spelled "Occurred" (2 r's)

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Colleen McCormack
Sent: Tuesday, January 22, 2019 10:31 AM
To: Bhanu Pothugunta
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

It is now working. What happened?

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Tuesday, January 22, 2019 10:26 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

It is working now. Can you please test and let me know if you are still having issues. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up “00 – Error occurred.”
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word “Occured”. It should be spelled “Occurred” (2 r’s)

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Tuesday, January 22, 2019 10:26 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

It is working now. Can you please test and let me know if you are still having issues. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up "00 – Error occurred."
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word "Occured". It should be spelled "Occurred" (2 r's)

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Tuesday, January 22, 2019 10:04 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: RE: ElectioNet UAT - 2FA Issue

Colleen,

We are working on this. Will update you once fixed. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up "00 – Error occurred."
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word "Occured". It should be spelled "Occurred" (2 r's)

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW

HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Colleen McCormack
Sent: Tuesday, January 22, 2019 9:46 AM
To: Bhanu Pothugunta
Cc: Daniel J Cloutier
Subject: ElectioNet UAT - 2FA Issue

Bhanu,
We cannot receive texts or emails from UAT. We receive the pop up "00 – Error occurred."
Could you please look into this for us?
I am copying Dan Cloutier so he may look at our end.
Please not the pop up has a misspelling of the word "Occured". It should be spelled "Occurred" (2 r's)

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Wednesday, January 16, 2019 8:12 AM
To: David Fournier
Subject: 2FA for ElectioNet

FYI

Thanks,
Dan

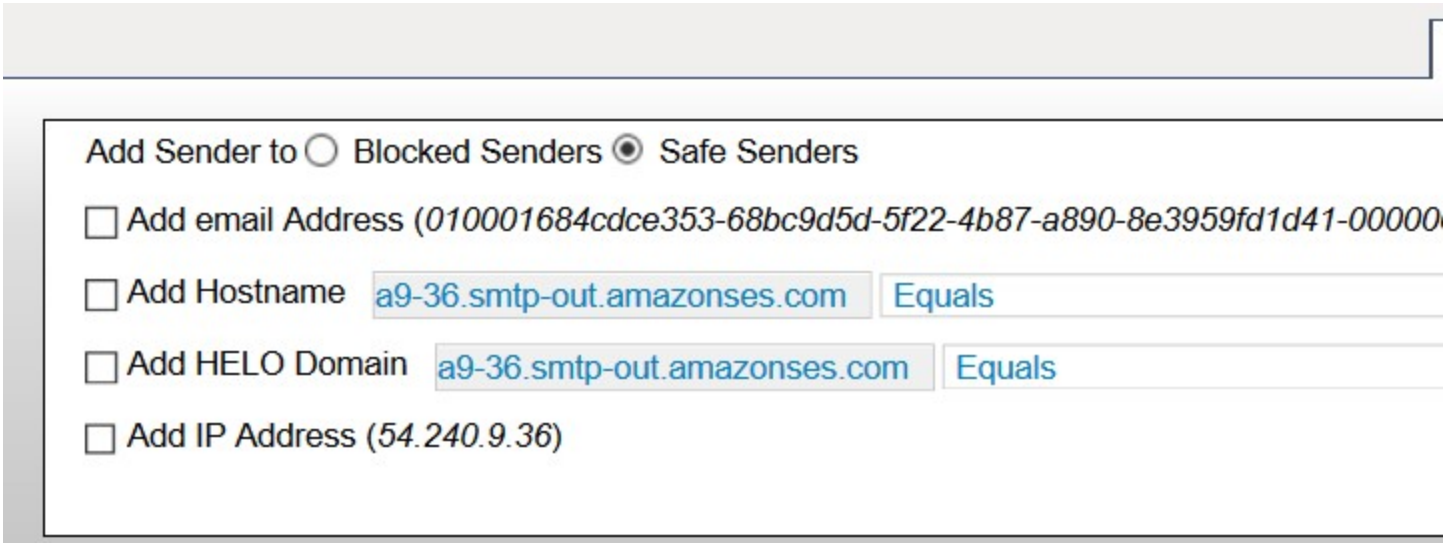
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, January 15, 2019 7:50 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: 2FA for ElectioNet

Keval,

We have deployed a very robust email scanning system that seems to be "catching" the 2FA emails. In order to "allow" these emails through, I need to add a rule. See the image below and indicate which items are static that the rule can allow these emails through.



Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Wednesday, January 16, 2019 8:11 AM
To: David Fournier
Subject: 2FA for ElectioNet

FYI

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>
Sent: Tuesday, January 15, 2019 9:07 AM
To: Keval Patel <Keval.Patel@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: RE: 2FA for ElectioNet

Good morning Dan. Could you please add "email-smtp.us-east-1.amazonaws.com" as the hostname on safe senders list.

Best Regards,
Ganesh Kumar Veerabathiran | Network Engineer
PCC Technology Inc., a subsidiary of GCR Inc. | pcctg.com
100 Northfield Dr. Suite 100 | Windsor, CT 06095
O. 860.580.7524

From: Keval Patel
Sent: Tuesday, January 15, 2019 8:22 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@sos.nh.gov>; Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: Re: 2FA for ElectioNet

Dan,

I've included Ganesh to call you on this. He is our IT manager and handles AWS email accounts. Thank you.

With Regards,
Keval Patel | Delivery Executive

Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Jan 15, 2019, at 6:50 AM, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Keval,
>
> We have deployed a very robust email scanning system that seems to be "catching" the 2FA emails. In order to "allow" these emails through, I need to add a rule. See the image below and indicate which items are static that the rule can allow these emails through.
>
> <image001.png>
>
> Thanks,
> *Dan*
>
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Wednesday, January 16, 2019 8:02 AM
To: Daniel J Cloutier
Subject: NH SVRS E-mail Verification

Dear DAN CLOUTIER,

This e-mail address is associated with the USER ID: HD-DCLOUT. Please click on the following link to verify this e-mail address.

The verification of this e-mail address will remain in effect until the e-mail address is changed or the user profile is deleted. Once you verify this e-mail address, you will be able to receive your authentication code using this e-mail address, in order to proceed logging into the NH SVRS. As a reminder, you will be required to authenticate your web browser periodically after the initial authentication. This e-mail address will be available for use each time you submit a request for an authentication code.

To verify this e-mail address, click here VERIFY EMAIL ADDRESS

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>
Sent: Tuesday, January 15, 2019 9:07 AM
To: Keval Patel; Daniel J Cloutier
Cc: Colleen McCormack; Anthony Stevens; Bhanu Pothugunta
Subject: RE: 2FA for ElectioNet

Good morning Dan. Could you please add "email-smtp.us-east-1.amazonaws.com" as the hostname on safe senders list.

Best Regards,
Ganesh Kumar Veerabathiran | Network Engineer
PCC Technology Inc., a subsidiary of GCR Inc. | pcctg.com
100 Northfield Dr. Suite 100 | Windsor, CT 06095
O. 860.580.7524

From: Keval Patel
Sent: Tuesday, January 15, 2019 8:22 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@sos.nh.gov>; Ganesh Veerabathiran <GaneshKumar.Veerabathiran@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: Re: 2FA for ElectioNet

Dan,

I've included Ganesh to call you on this. He is our IT manager and handles AWS email accounts. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Jan 15, 2019, at 6:50 AM, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Keval,
>
> We have deployed a very robust email scanning system that seems to be "catching" the 2FA emails. In order to "allow" these emails through, I need to add a rule. See the image below and indicate which items are static that the rule can allow these emails through.
>
> <image001.png>
>
> Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, January 15, 2019 8:22 AM
To: Daniel J Cloutier
Cc: Colleen McCormack; Anthony Stevens; Ganesh Veerabathiran; Bhanu Pothugunta
Subject: Re: 2FA for ElectioNet

Dan,

I've included Ganesh to call you on this. He is our IT manager and handles AWS email accounts. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Jan 15, 2019, at 6:50 AM, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

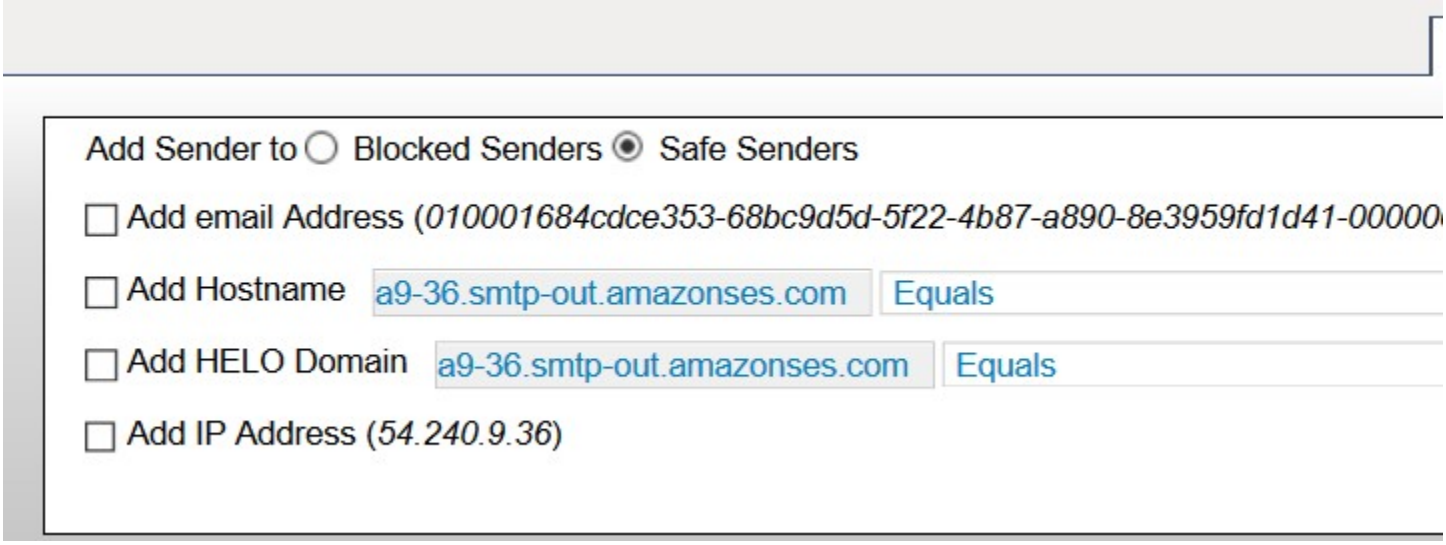
> Keval,
>
> We have deployed a very robust email scanning system that seems to be "catching" the 2FA emails. In order to "allow" these emails through, I need to add a rule. See the image below and indicate which items are static that the rule can allow these emails through.
>
> <image001.png>
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, January 15, 2019 7:50 AM
To: Keval Patel
Cc: Colleen McCormack; Anthony Stevens
Subject: 2FA for ElectioNet

Keval,

We have deployed a very robust email scanning system that seems to be "catching" the 2FA emails. In order to "allow" these emails through, I need to add a rule. See the image below and indicate which items are static that the rule can allow these emails through.



Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Wednesday, January 9, 2019 1:49 PM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DANIEL CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID DCLOUTIER. Enter the authentication code that appears below to verify your account.

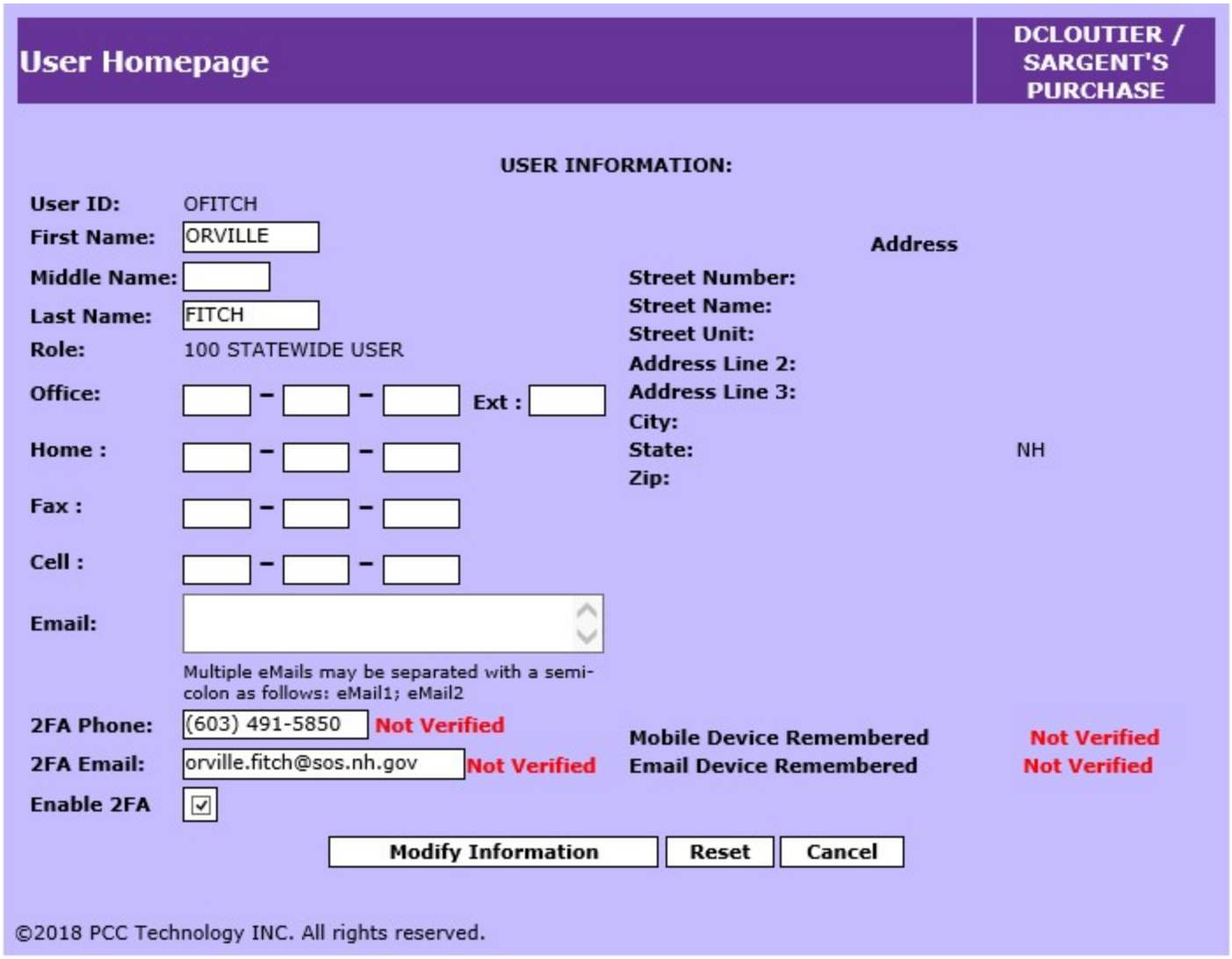
The authentication code for USER ID DCLOUTIER is: 394535.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Wednesday, January 9, 2019 1:52 PM
To: Jeffrey King
Subject: 2FA



User Homepage | **DCLOUTIER / SARGENT'S PURCHASE**

USER INFORMATION:

User ID: OFITCH
First Name: ORVILLE
Middle Name:
Last Name: FITCH
Role: 100 STATEWIDE USER
Office: – – Ext :
Home : – –
Fax : – –
Cell : – –
Email:

Multiple eMails may be separated with a semi-colon as follows: eMail1; eMail2

2FA Phone: (603) 491-5850 Not Verified
2FA Email: orville.fitch@sos.nh.gov Not Verified
Enable 2FA ☑

Address

Street Number:
Street Name:
Street Unit:
Address Line 2:
Address Line 3:
City:
State: NH
Zip:

Mobile Device Remembered Not Verified
Email Device Remembered Not Verified

Modify Information | Reset | Cancel

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Thursday, December 6, 2018 7:13 AM
To: Daniel J Cloutier
Subject: NH SVRS Authentication Code

Dear DAN CLOUTIER,

You are receiving this email because an authentication request was submitted in the NH SVRS for USER ID HD-DCLOUT. Enter the authentication code that appears below to verify your account.

The authentication code for USER ID HD-DCLOUT is: 975531.

Do not forward or give this code to anyone. If you did not initiate an authentication request, it is possible that someone else is trying to access your account. Please contact your State Administrator to ensure your account is safe.

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: NHVotes@sos.nh.gov
Sent: Thursday, December 6, 2018 7:11 AM
To: Daniel J Cloutier
Subject: NH SVRS E-mail Verification

Dear DAN CLOUTIER,

This e-mail address is associated with the USER ID: HD-DCLOUT. Please click on the following link to verify this e-mail address.

The verification of this e-mail address will remain in effect until the e-mail address is changed or the user profile is deleted. Once you verify this e-mail address, you will be able to receive your authentication code using this e-mail address, in order to proceed logging into the NH SVRS. As a reminder, you will be required to authenticate your web browser periodically after the initial authentication. This e-mail address will be available for use each time you submit a request for an authentication code.

To verify this e-mail address, click here VERIFY EMAIL ADDRESS

Sincerely,
Elections Division
Office of the New Hampshire Secretary of State

Daniel J Cloutier

From: Colleen McCormack
Sent: Monday, December 3, 2018 4:22 PM
To: Keval Patel; Daniel J Cloutier
Cc: Bhanu Pothugunta; Anil Kumar Prathipati
Subject: RE: NH ElectioNet - 2FA Updates

Keval,
Thank you for your explanation.
I am copying Dan Cloutier if he has any questions.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Monday, December 03, 2018 4:16 PM
To: Colleen McCormack
Cc: Bhanu Pothugunta; Anil Kumar Prathipati
Subject: Re: NH ElectioNet - 2FA Updates

Text message will have the URL with encrypted token. We are not showing User ID any more. We cannot show button as part of text message. Please let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Dec 3, 2018, at 4:12 PM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

Bhanu,
We have completed 2 android verifications for the email and text and they passed.
Anthony has an iPhone and he was able to verify the text. He was not able to verify his SOS email address from his computer. I will check into it with Dan tomorrow to see if something is blocking the email to an SOS address.

The text verification still has the complete URL address. This needs to be masked in the same manner to appear as the email URL button.

I will continue to test the 2FA tomorrow.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Bhanu Pothugunta [mailto:bhanu.pothugunta@pcctg.com]
Sent: Monday, December 03, 2018 11:48 AM
To: Colleen McCormack
Cc: Keval Patel; Anil Kumar Prathipati
Subject: RE: NH ElectioNet - 2FA Updates

Colleen,

We have fixed the items in the document and verification link issue in android. Please review in UAT and let us know your comments. Thank You.

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, November 27, 2018 12:26 PM

To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Subject: NH ElectioNet - 2FA Updates

Bhanu,
I have attached the updates needed in the 2FA process.
I did not add the ticket to TAS, so I cannot see the appropriate ticket number to report any issues. Could you tell me the ticket number, so I may document it.
Let me know if you have any questions.

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, November 27, 2018 11:36 AM
To: Colleen McCormack
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: RE: 2FA - Verifying Cell Phone Number

Dan,

As discussed, we'll remove user information from the verification link and keep the encoded token number only. We'll update you once we move the change in UAT. Please let me know if any questions. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Sent: Tuesday, November 27, 2018 10:38 AM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>
Subject: RE: 2FA - Verifying Cell Phone Number

Perfect.

Thank You,
Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:37 AM

To: Colleen McCormack
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: Re: 2FA - Verifying Cell Phone Number

Ok. We'll call Dan at his direct line. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:35 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> It is a good time for us both.
> Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:35 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: Re: 2FA - Verifying Cell Phone Number

11am?

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:34 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval,
> I am forwarding your email to Dan.
> Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Bhanu,
> Can Dan and I call you back?

He wants to discuss how the verification is coming back into ElectioNet?

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Colleen McCormack
Sent: Tuesday, November 27, 2018 10:38 AM
To: Keval Patel
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: RE: 2FA - Verifying Cell Phone Number

Perfect.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:37 AM
To: Colleen McCormack
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: Re: 2FA - Verifying Cell Phone Number

Ok. We'll call Dan at his direct line. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:35 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> It is a good time for us both.
> Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:35 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: Re: 2FA - Verifying Cell Phone Number

11am?

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:34 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval,
> I am forwarding your email to Dan.
> Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301

Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Bhanu,
> Can Dan and I call you back?
> He wants to discuss how the verification is coming back into ElectioNet?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

at (603) 271-8241 or reply to nhvotes@sos.nh.gov if you are not the intended recipient and destroy all copies of this electronic message and any attachments.

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, November 27, 2018 10:37 AM
To: Colleen McCormack
Cc: Daniel J Cloutier; Bhanu Pothugunta; Anil Kumar Prathipati
Subject: Re: 2FA - Verifying Cell Phone Number

Ok. We'll call Dan at his direct line. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:35 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> It is a good time for us both.
> Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:35 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: Re: 2FA - Verifying Cell Phone Number

11am?

With Regards,

Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:34 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval,
> I am forwarding your email to Dan.
> Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

Bhanu,
Can Dan and I call you back?
He wants to discuss how the verification is coming back into ElectioNet?

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Colleen McCormack
Sent: Tuesday, November 27, 2018 10:36 AM
To: Keval Patel
Cc: Daniel J Cloutier
Subject: RE: 2FA - Verifying Cell Phone Number

It is a good time for us both.
Thank you.

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:35 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: Re: 2FA - Verifying Cell Phone Number

11am?

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:34 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval,
> I am forwarding your email to Dan.

Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Bhanu,
> Can Dan and I call you back?
> He wants to discuss how the verification is coming back into ElectioNet?

Thank You,
Colleen
Colleen E. McCormack
HAVA

Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, November 27, 2018 10:35 AM
To: Colleen McCormack
Cc: Daniel J Cloutier
Subject: Re: 2FA - Verifying Cell Phone Number

11am?

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:34 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval,
> I am forwarding your email to Dan.
> Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Bhanu,
> Can Dan and I call you back?
> He wants to discuss how the verification is coming back into ElectioNet?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Colleen McCormack
Sent: Tuesday, November 27, 2018 10:34 AM
To: Daniel J Cloutier; Keval Patel
Subject: FW: 2FA - Verifying Cell Phone Number

Keval,
I am forwarding your email to Dan.
Do you know a time for the call?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Tuesday, November 27, 2018 10:33 AM
To: Colleen McCormack
Cc: Bhanu Pothugunta
Subject: Re: 2FA - Verifying Cell Phone Number

Colleen,

I'll call you today to discuss on this. Thank you.

With Regards,
Keval Patel | Delivery Executive
Elections and Ethics Product Support
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Nov 27, 2018, at 10:31 AM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

Bhanu,
Can Dan and I call you back?
He wants to discuss how the verification is coming back into ElectioNet?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Amazon Web Services <no-reply-aws@amazon.com>
Sent: Monday, October 15, 2018 11:29 AM
To: NHVotes
Subject: Amazon Web Services – Email Address Verification Request in region US East (N. Virginia)

Dear Amazon Web Services Customer,

We have received a request to authorize this email address for use with Amazon SES and Amazon Pinpoint in region US East (N. Virginia). If you requested this verification, please go to the following URL to confirm that you are authorized to use this email address:

https://email-verification.us-east-1.amazonaws.com/?Context=462410914576&X-Amz-Date=20181015T152929Z&Identity.IdentityName=NHVotes%40sos.nh.gov&X-Amz-Algorithm=AWS4-HMAC-SHA256&Identity.IdentityType=EmailAddress&X-Amz-SignedHeaders=host&X-Amz-Credential=AKIAJRRY6IQWNCSWXCTA%2F20181015%2Fus-east-1%2Fses%2Faws4_request&Operation=ConfirmVerification&Namespace=Bacon&X-Amz-Signature=e165725e0ae8c637c5b36fd25e8b92ecf486559d8b323cce7a817a64c37d6084

Your request will not be processed unless you confirm the address using this URL. This link expires 24 hours after your original verification request.

If you did NOT request to verify this email address, do not click on the link. Please note that many times, the situation isn't a phishing attempt, but either a misunderstanding of how to use our service, or someone setting up email-sending capabilities on your behalf as part of a legitimate service, but without having fully communicated the procedure first. If you are still concerned, please forward this notification to aws-email-domain-verification@amazon.com and let us know in the forward that you did not request the verification.

To learn more about sending email from Amazon Web Services, please refer to the Amazon SES Developer Guide at http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html and Amazon Pinpoint Developer Guide at http://docs.aws.amazon.com/pinpoint/latest/userguide/welcome.html.

Sincerely,

The Amazon Web Services Team.

Daniel J Cloutier

From: Help Desk Services <helpdesk@nh.gov>
Sent: Wednesday, October 10, 2018 11:14 AM
To: Daniel J Cloutier
Subject: The below work request received by the DoIT Help Desk has been completed. ISSUE= 1134369 PROJ=1
Attachments: ports-services-request-form (1).doc

Importance: High

When replying, type your text above this line.

Notification of Issue Escalation

Description:
Dan C reports successful testing. closing.

NOTE - Please do not reply to this unless you want to REOPEN the completed work order!!

The below work request received by the DoIT Help Desk has been completed.

Ticket #: 1134369
Summary: Port Opening Request from DMZ

If you feel this issue has not been resolved to your satisfaction, please contact:

DOIT Central Help Desk (603) 271-7555.
NHSLC Help Desk (603) 230-7000.

Your request will be reviewed and reopened if necessary.

Survey: Please take a moment to rate the service you received by completing a Survey

We look forward to servicing your needs in the future.

State of New Hampshire
Department of Information Technology

Visit us at: DoIT our intranet website

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Wednesday, October 10, 2018 11:05 AM
To: 'Pomeroy, Jeffrey'; Christopher Bentzler; Scott C. Caveney; David Fournier
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Vendor has verified connectivity. Ticket success once again. You are amazing.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Pomeroy, Jeffrey <Jeffrey.Pomeroy@doit.nh.gov>
Sent: Tuesday, October 9, 2018 2:12 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Christopher Bentzler <Christopher.Bentzler@sos.nh.gov>; Scott C. Caveney <Scott.Caveney@sos.nh.gov>; David Fournier <David.Fournier@SOS.NH.GOV>
Subject: FW: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Updates made for these. Please test and let me know.

From: Help Desk Services [mailto:helpdesk@nh.gov]
Sent: Tuesday, October 09, 2018 12:57 PM
To: Pomeroy, Jeffrey
Subject: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

When replying, type your text above this line.

Notification of Issue Change

Workspace: Help Desk
Issue: Port Opening Request from DMZ
Issue Number: 1134369

Priority:	5	**Status:**	Assigned
Date:	2018-10-09	**Time:**	12:57:16
Creation Date:	2018-10-09	**Creation Time:**	11:29:47
Created By:	daniel.cloutier@sos.nh.gov		

Click here to view Issue in Browser

Description:
Entered on 2018-10-09 at 12:57:16 EDT (GMT-0400) by David Hunger:
Assigning

Entered on 2018-10-09 at 12:01:44 EDT (GMT-0400) by Gerard Wallace:
ITSG is good with this request, have added Port request form.

Entered on 2018-10-09 at 11:36:07 EDT (GMT-0400) by David Hunger:
To ITSG for review regarding destination IP.

Entered on 2018-10-09 at 11:33:38 EDT (GMT-0400) by Bonnie Hannagan:
Assigned to OPS-Netops

Entered on 2018-10-09 at 11:29:47 EDT (GMT-0400) by daniel.cloutier@sos.nh.gov:
The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Current Assignees: Jeff Pomeroy

CC(s): (permanent) Christopher.Bentzler@sos.nh.gov, David.Fournier@SOS.NH.GOV, Scott.Caveney@sos.nh.gov

Issue Information:

Impact:	Medium	**Urgency:**	Low
Status Detail Assigned:	Route	**Status Request:**	No
Problem Type:	Connectivity	**Category:**	ACL Change
Issue:	Port Modification	**Technician Assigned:**	Jeffrey Pomeroy
Team:	NETOPS	**Sub-Division:**	Network Operations
Division:	Operations	**Supported Agency:**	Secretary of State
Remote Assistance via:	None	**SLA Due Date:**	2018-10-19 11:29
SLA Response Time:	2018-10-11 11:29	**Submission Tracking:**	Email
SLA Breached:	No	**WorkOrderNumber:**	1134369
HDS Processed:	Bonnie.A.Hannagan		

Contact Information:

Last Name:	Cloutier	**First Name:**	Daniel

Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Phone:**	603-271-0001
User ID:	Daniel.Cloutier	**Email Address:**	daniel.cloutier@sos.nh.gov
Address Line 1:	107 North Main St	**City/Town:**	Concord
Site:	State House	**RSS Support Team:**	None -Self Supported
Agency:	Secretary of State		

Attachments: ports-services-request-form (1).doc

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Wednesday, October 10, 2018 7:55 AM
To: Daniel J Cloutier
Cc: Bhanu Pothugunta; Anil Kumar Prathipati; Colleen McCormack
Subject: Re: Request to enable ports to generate TFA

Dan,

Good morning. We are able to access our proxy server to send SMS and Email through AWS. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Oct 9, 2018, at 4:05 PM, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> All servers should now have access to the destination you have requested. Please test and let me know the outcome.
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> ---
>
> **From:** Daniel J Cloutier
> **Sent:** Tuesday, October 9, 2018 11:24 AM
> **To:** 'Keval Patel' <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
> **Cc:** Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
> **Subject:** RE: Request to enable ports to generate TFA
>
> Keval & Bhanu,
>
> The 10.144.x.x servers already have access. I will request access for the dmz servers.
>
> Thanks,

Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT

10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 4:35 PM
To: Daniel J Cloutier; Bhanu Pothugunta
Cc: Anil Kumar Prathipati; Colleen McCormack
Subject: RE: Request to enable ports to generate TFA

Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Tuesday, October 9, 2018 4:13 PM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

199.192.7.134 for the dmz servers and 199.192.1.120 for the internal servers

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 4:07 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan, we also need a public IP address for the below server to whitelist on our side to allow access to proxy server. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Tuesday, October 9, 2018 4:05 PM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

All servers should now have access to the destination you have requested. Please test and let me know the outcome.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 11:24 AM
To: 'Keval Patel' <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Keval & Bhanu,

The 10.144.x.x servers already have access. I will request access for the dmz servers.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 4:13 PM
To: 'Keval Patel'; Bhanu Pothugunta
Cc: Anil Kumar Prathipati; Colleen McCormack
Subject: RE: Request to enable ports to generate TFA

199.192.7.134 for the dmz servers and 199.192.1.120 for the internal servers

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 4:07 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan, we also need a public IP address for the below server to whitelist on our side to allow access to proxy server. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Tuesday, October 9, 2018 4:05 PM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

All servers should now have access to the destination you have requested. Please test and let me know the outcome.

Thanks,
Dan
Daniel J Cloutier

Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 11:24 AM
To: 'Keval Patel' <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Keval & Bhanu,

The 10.144.x.x servers already have access. I will request access for the dmz servers.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack

<Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 4:07 PM
To: Daniel J Cloutier; Bhanu Pothugunta
Cc: Anil Kumar Prathipati; Colleen McCormack
Subject: RE: Request to enable ports to generate TFA

Dan, we also need a public IP address for the below server to whitelist on our side to allow access to proxy server. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Tuesday, October 9, 2018 4:05 PM
To: Keval Patel <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

All servers should now have access to the destination you have requested. Please test and let me know the outcome.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 11:24 AM
To: 'Keval Patel' <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Keval & Bhanu,

The 10.144.x.x servers already have access. I will request access for the dmz servers.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server

10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 4:05 PM
To: 'Keval Patel'; 'Bhanu Pothugunta'
Cc: 'Anil Kumar Prathipati'; Colleen McCormack
Subject: RE: Request to enable ports to generate TFA

All servers should now have access to the destination you have requested. Please test and let me know the outcome.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 11:24 AM
To: 'Keval Patel' <Keval.Patel@pcctg.com>; Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Keval & Bhanu,

The 10.144.x.x servers already have access. I will request access for the dmz servers.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Pomeroy, Jeffrey <Jeffrey.Pomeroy@doit.nh.gov>
Sent: Tuesday, October 9, 2018 2:12 PM
To: Daniel J Cloutier; Christopher Bentzler; Scott C. Caveney; David Fournier
Subject: FW: Port Opening Request from DMZ ISSUE=1134369 PROJ=1
Attachments: ports-services-request-form (1).doc

Updates made for these. Please test and let me know.

From: Help Desk Services [mailto:helpdesk@nh.gov]
Sent: Tuesday, October 09, 2018 12:57 PM
To: Pomeroy, Jeffrey
Subject: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

When replying, type your text above this line.

Notification of Issue Change

Workspace: Help Desk
Issue: Port Opening Request from DMZ
Issue Number: 1134369

Priority:	5	**Status:**	Assigned
Date:	2018-10-09	**Time:**	12:57:16
Creation Date:	2018-10-09	**Creation Time:**	11:29:47
Created By:	daniel.cloutier@sos.nh.gov		

Click here to view Issue in Browser

Description:
Entered on 2018-10-09 at 12:57:16 EDT (GMT-0400) by David Hunger:
Assigning

Entered on 2018-10-09 at 12:01:44 EDT (GMT-0400) by Gerard Wallace:
ITSG is good with this request, have added Port request form.

Entered on 2018-10-09 at 11:36:07 EDT (GMT-0400) by David Hunger:
To ITSG for review regarding destination IP.

Entered on 2018-10-09 at 11:33:38 EDT (GMT-0400) by Bonnie Hannagan:
Assigned to OPS-Netops

Entered on 2018-10-09 at 11:29:47 EDT (GMT-0400) by daniel.cloutier@sos.nh.gov:
The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Current Assignees: Jeff Pomeroy

CC(s): (permanent) Christopher.Bentzler@sos.nh.gov, David.Fournier@SOS.NH.GOV, Scott.Caveney@sos.nh.gov

Issue Information:

Impact:	Medium	**Urgency:**	Low
Status Detail Assigned:	Route	**Status Request:**	No
Problem Type:	Connectivity	**Category:**	ACL Change
Issue:	Port Modification	**Technician Assigned:**	Jeffrey Pomeroy
Team:	NETOPS	**Sub-Division:**	Network Operations
Division:	Operations	**Supported Agency:**	Secretary of State
Remote Assistance via:	None	**SLA Due Date:**	2018-10-19 11:29
SLA Response Time:	2018-10-11 11:29	**Submission Tracking:**	Email
SLA Breached:	No	**WorkOrderNumber:**	1134369
HDS Processed:	Bonnie.A.Hannagan		

Contact Information:

Last Name:	Cloutier	**First Name:**	Daniel
Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Phone:**	603-271-0001
User ID:	Daniel.Cloutier	**Email Address:**	daniel.cloutier@sos.nh.gov
Address Line 1:	107 North Main St	**City/Town:**	Concord
Site:	State House	**RSS Support Team:**	None -Self Supported
Agency:	Secretary of State		

Attachments: ports-services-request-form (1).doc

Daniel J Cloutier

From: Wallace, Gerard <Gerard.Wallace@doit.nh.gov>
Sent: Tuesday, October 9, 2018 12:32 PM
To: Daniel J Cloutier
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

I was wondering, since a lookup on that address resolves differently.

Microsoft Windows [Version 10.0.16299.611]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\>nslookup http://electionproxy.pcctg.net
Server: sopsgrandc5.granite.nhroot.int
Address: 10.144.35.71

Non-authoritative answer:
Name: http://electionproxy.pcctg.net
Address: 96.127.55.121

C:\>

Gerard E. Wallace, Security Specialist
New Hampshire Cyber Integration Center (NH-CIC)
NH Department of Information Technology
110 Smokey Bear Blvd
Concord NH 03301
Direct Line: 227-0085
NH-CIC: 603-227-0087
New Hampshire Cyber Integration Center (NH-CIC): NH-CIC@doit.nh.gov

---

From: Daniel J Cloutier [mailto:Daniel.Cloutier@sos.nh.gov]
Sent: Tuesday, October 9, 2018 12:12 PM
To: Wallace, Gerard
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

… but I suppose they could have an Amazon cloud server that they are renting …

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 12:11 PM
To: 'Wallace, Gerard' <Gerard.Wallace@doit.nh.gov>
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Negative. It is our vendor: URL: http://electionproxy.pcctg.net/

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Wallace, Gerard <Gerard.Wallace@doit.nh.gov>
Sent: Tuesday, October 9, 2018 12:06 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: FW: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Is this an Amazon address? 52.61.5.151

Jerry

Gerard E. Wallace, Security Specialist
New Hampshire Cyber Integration Center (NH-CIC)
NH Department of Information Technology
110 Smokey Bear Blvd
Concord NH 03301
Direct Line: 227-0085
NH-CIC: 603-227-0087
New Hampshire Cyber Integration Center (NH-CIC): NH-CIC@doit.nh.gov

From: Help Desk Services [mailto:helpdesk@nh.gov]
Sent: Tuesday, October 9, 2018 11:36 AM
To: Wallace, Gerard
Subject: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

When replying, type your text above this line.

Notification of Issue Change

Workspace: Help Desk

Issue: Port Opening Request from DMZ
Issue Number: 1134369

Priority:	5	**Status:**	Open
Date:	2018-10-09	**Time:**	11:36:08
Creation Date:	2018-10-09	**Creation Time:**	11:29:47
Created By:	daniel.cloutier@sos.nh.gov		

Click here to view Issue in Browser

Description:
Entered on 2018-10-09 at 11:36:07 EDT (GMT-0400) by David Hunger:
To ITSG for review regarding destination IP.

Entered on 2018-10-09 at 11:33:38 EDT (GMT-0400) by Bonnie Hannagan:
Assigned to OPS-Netops

Entered on 2018-10-09 at 11:29:47 EDT (GMT-0400) by daniel.cloutier@sos.nh.gov:
The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Current Assignees: ITSG

CC(s): (permanent) Christopher.Bentzler@sos.nh.gov, David.Fournier@SOS.NH.GOV, Scott.Caveney@sos.nh.gov

Issue Information:

Impact:	Medium	**Urgency:**	Low
Status Request:	No	**Problem Type:**	Connectivity
Category:	ACL Change	**Issue:**	Port Modification
Technician Assigned:	# ITSG	**Team:**	ITSG
Sub-Division:	ITSG	**Division:**	ITSG
Supported Agency:	Secretary of State	**SLA Due Date:**	2018-10-19 11:29
SLA Response Time:	2018-10-11 11:29	**Submission Tracking:**	Email
WorkOrderNumber:	1134369	**HDS Processed:**	Bonnie.A.Hannagan

Contact Information:

Last Name:	Cloutier	**First Name:**	Daniel
Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Phone:**	603-271-0001
User ID:	Daniel.Cloutier	**Email Address:**	daniel.cloutier@sos.nh.gov
Address Line 1:	107 North Main St	**City/Town:**	Concord
Site:	State House	**RSS Support Team:**	None -Self Supported
Agency:	Secretary of State		

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 12:12 PM
To: 'Wallace, Gerard'
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

… but I suppose they could have an Amazon cloud server that they are renting …

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 12:11 PM
To: 'Wallace, Gerard' <Gerard.Wallace@doit.nh.gov>
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Negative. It is our vendor: URL: http://electionproxy.pcctg.net/

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Wallace, Gerard <Gerard.Wallace@doit.nh.gov>
Sent: Tuesday, October 9, 2018 12:06 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: FW: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Is this an Amazon address? 52.61.5.151

Jerry

Gerard E. Wallace, Security Specialist
New Hampshire Cyber Integration Center (NH-CIC)

NH Department of Information Technology
110 Smokey Bear Blvd
Concord NH 03301
Direct Line: 227-0085
NH-CIC: 603-227-0087
New Hampshire Cyber Integration Center (NH-CIC): NH-CIC@doit.nh.gov

From: Help Desk Services [mailto:helpdesk@nh.gov]
Sent: Tuesday, October 9, 2018 11:36 AM
To: Wallace, Gerard
Subject: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

When replying, type your text above this line.

Notification of Issue Change

Workspace: Help Desk
Issue: Port Opening Request from DMZ
Issue Number: 1134369

Priority:	5	**Status:**	Open
Date:	2018-10-09	**Time:**	11:36:08
Creation Date:	2018-10-09	**Creation Time:**	11:29:47
Created By:	daniel.cloutier@sos.nh.gov		

Click here to view Issue in Browser

Description:
Entered on 2018-10-09 at 11:36:07 EDT (GMT-0400) by David Hunger:
To ITSG for review regarding destination IP.

Entered on 2018-10-09 at 11:33:38 EDT (GMT-0400) by Bonnie Hannagan:
Assigned to OPS-Netops

Entered on 2018-10-09 at 11:29:47 EDT (GMT-0400) by daniel.cloutier@sos.nh.gov:
The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Current Assignees: ITSG

CC(s): (permanent) Christopher.Bentzler@sos.nh.gov, David.Fournier@SOS.NH.GOV, Scott.Caveney@sos.nh.gov

Issue Information:

Impact:	Medium	**Urgency:**	Low
Status Request:	No	**Problem Type:**	Connectivity
Category:	ACL Change	**Issue:**	Port Modification
Technician Assigned:	# ITSG	**Team:**	ITSG
Sub-Division:	ITSG	**Division:**	ITSG
Supported Agency:	Secretary of State	**SLA Due Date:**	2018-10-19 11:29
SLA Response Time:	2018-10-11 11:29	**Submission Tracking:**	Email
WorkOrderNumber:	1134369	**HDS Processed:**	Bonnie.A.Hannagan

Contact Information:

Last Name:	Cloutier	**First Name:**	Daniel
Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Phone:**	603-271-0001
User ID:	Daniel.Cloutier	**Email Address:**	daniel.cloutier@sos.nh.gov
Address Line 1:	107 North Main St	**City/Town:**	Concord
Site:	State House	**RSS Support Team:**	None -Self Supported
Agency:	Secretary of State		

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 12:11 PM
To: 'Wallace, Gerard'
Subject: RE: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Negative. It is our vendor: URL: http://electionproxy.pcctg.net/

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Wallace, Gerard <Gerard.Wallace@doit.nh.gov>
Sent: Tuesday, October 9, 2018 12:06 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: FW: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Is this an Amazon address? 52.61.5.151

Jerry

Gerard E. Wallace, Security Specialist
New Hampshire Cyber Integration Center (NH-CIC)
NH Department of Information Technology
110 Smokey Bear Blvd
Concord NH 03301
Direct Line: 227-0085
NH-CIC: 603-227-0087
New Hampshire Cyber Integration Center (NH-CIC): NH-CIC@doit.nh.gov

From: Help Desk Services [mailto:helpdesk@nh.gov]
Sent: Tuesday, October 9, 2018 11:36 AM
To: Wallace, Gerard
Subject: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

When replying, type your text above this line.

Notification of Issue Change

Workspace: Help Desk
Issue: Port Opening Request from DMZ
Issue Number: 1134369

Priority:	5	**Status:**	Open
Date:	2018-10-09	**Time:**	11:36:08
Creation Date:	2018-10-09	**Creation Time:**	11:29:47
Created By:	daniel.cloutier@sos.nh.gov		

Click here to view Issue in Browser

Description:
Entered on 2018-10-09 at 11:36:07 EDT (GMT-0400) by David Hunger:
To ITSG for review regarding destination IP.

Entered on 2018-10-09 at 11:33:38 EDT (GMT-0400) by Bonnie Hannagan:
Assigned to OPS-Netops

Entered on 2018-10-09 at 11:29:47 EDT (GMT-0400) by daniel.cloutier@sos.nh.gov:
The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Current Assignees: ITSG

CC(s): (permanent) Christopher.Bentzler@sos.nh.gov, David.Fournier@SOS.NH.GOV, Scott.Caveney@sos.nh.gov

Issue Information:

Impact:	Medium	**Urgency:**	Low
Status Request:	No	**Problem Type:**	Connectivity
Category:	ACL Change	**Issue:**	Port Modification
Technician Assigned:	# ITSG	**Team:**	ITSG
Sub-Division:	ITSG	**Division:**	ITSG
Supported Agency:	Secretary of State	**SLA Due Date:**	2018-10-19 11:29
SLA Response Time:	2018-10-11 11:29	**Submission Tracking:**	Email
WorkOrderNumber:	1134369	**HDS Processed:**	Bonnie.A.Hannagan

Contact Information:

Last Name:	Cloutier	**First Name:**	Daniel
Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Phone:**	603-271-0001
User ID:	Daniel.Cloutier	**Email Address:**	daniel.cloutier@sos.nh.gov
Address Line 1:	107 North Main St	**City/Town:**	Concord
Site:	State House	**RSS Support Team:**	None -Self Supported
Agency:	Secretary of State		

Daniel J Cloutier

From: Wallace, Gerard <Gerard.Wallace@doit.nh.gov>
Sent: Tuesday, October 9, 2018 12:06 PM
To: Daniel J Cloutier
Subject: FW: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

Is this an Amazon address? 52.61.5.151

Jerry

Gerard E. Wallace, Security Specialist
New Hampshire Cyber Integration Center (NH-CIC)
NH Department of Information Technology
110 Smokey Bear Blvd
Concord NH 03301
Direct Line: 227-0085
NH-CIC: 603-227-0087
New Hampshire Cyber Integration Center (NH-CIC): NH-CIC@doit.nh.gov

From: Help Desk Services [mailto:helpdesk@nh.gov]
Sent: Tuesday, October 9, 2018 11:36 AM
To: Wallace, Gerard
Subject: Port Opening Request from DMZ ISSUE=1134369 PROJ=1

When replying, type your text above this line.

Notification of Issue Change

Workspace: Help Desk
Issue: Port Opening Request from DMZ
Issue Number: 1134369

Priority:	5	**Status:**	Open
Date:	2018-10-09	**Time:**	11:36:08
Creation Date:	2018-10-09	**Creation Time:**	11:29:47
Created By:	daniel.cloutier@sos.nh.gov		

Click here to view Issue in Browser

Description:
Entered on 2018-10-09 at 11:36:07 EDT (GMT-0400) by David Hunger:
To ITSG for review regarding destination IP.

Entered on 2018-10-09 at 11:33:38 EDT (GMT-0400) by Bonnie Hannagan:
Assigned to OPS-Netops

Entered on 2018-10-09 at 11:29:47 EDT (GMT-0400) by daniel.cloutier@sos.nh.gov:
The Department of State requests the following servers in the data center DMZ be allowed to

communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Current Assignees: ITSG

CC(s): (permanent) Christopher.Bentzler@sos.nh.gov, David.Fournier@SOS.NH.GOV, Scott.Caveney@sos.nh.gov

Issue Information:

Impact:	Medium	**Urgency:**	Low
Status Request:	No	**Problem Type:**	Connectivity
Category:	ACL Change	**Issue:**	Port Modification
Technician Assigned:	# ITSG	**Team:**	ITSG
Sub-Division:	ITSG	**Division:**	ITSG
Supported Agency:	Secretary of State	**SLA Due Date:**	2018-10-19 11:29
SLA Response Time:	2018-10-11 11:29	**Submission Tracking:**	Email
WorkOrderNumber:	1134369	**HDS Processed:**	Bonnie.A.Hannagan

Contact Information:

Last Name:	Cloutier	**First Name:**	Daniel
Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Phone:**	603-271-0001
User ID:	Daniel.Cloutier	**Email Address:**	daniel.cloutier@sos.nh.gov
Address Line 1:	107 North Main St	**City/Town:**	Concord
Site:	State House	**RSS Support Team:**	None -Self Supported
Agency:	Secretary of State		

Daniel J Cloutier

From: Help Desk Services <helpdesk@nh.gov>
Sent: Tuesday, October 9, 2018 11:30 AM
To: Daniel J Cloutier
Subject: The below work request Port Opening Request from DMZ received by the DoIT Help Desk has been logged as ISSUE=1134369 PROJ=1

Importance: High

When replying, type your text above this line.

Notification of Issue Escalation

Your service request regarding Port Opening Request from DMZ has been logged as 1134369 .

If CHANGES to your ISSUE have occurred please SELECT REPLY and UPDATE the Help Desk
by entering the NEW INFORMATION in the REPLY email message area.
Issue: Port Opening Request from DMZ
Issue Number: 1134369

Status: Request

Description:
The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source Destination Ports
10.12.20.102 52.61.5.151 TCP/80 & 443
10.12.20.103 52.61.5.151 TCP/80 & 443
10.12.20.104 52.61.5.151 TCP/80 & 443

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Contact Information:

Last Name: Cloutier **First Name:** Daniel

Email Address:	daniel.cloutier@sos.nh.gov	**Phone:**	603-271-0001
Site:	State House	**Agency:**	Secretary of State
Middle:	J	**Position-Title:**	Assistant Secretary of State
Bureau/Division:	IT Office	**Address Line 1:**	107 North Main St
City/Town:	Concord		

Please verify the above contact information we currently have on file for you. If it is incorrect please reply above the line with the correct contact information.

Thank you

Help Desk Services

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 11:27 AM
To: 'HelpDesk@doit.nh.gov'
Cc: Scott C. Caveney; David Fournier; Christopher Bentzler
Subject: Port Opening Request from DMZ

The Department of State requests the following servers in the data center DMZ be allowed to communicate to a proxy server in order to facilitate our two-factor authentication protocol for our election related servers:

Source	Destination	Ports
10.12.20.102	52.61.5.151	TCP/80 & 443
10.12.20.103	52.61.5.151	TCP/80 & 443
10.12.20.104	52.61.5.151	TCP/80 & 443

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, October 9, 2018 11:24 AM
To: 'Keval Patel'; Bhanu Pothugunta
Cc: Anil Kumar Prathipati; Colleen McCormack
Subject: RE: Request to enable ports to generate TFA

Keval & Bhanu,

The 10.144.x.x servers already have access. I will request access for the dmz servers.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Tuesday, October 9, 2018 10:43 AM
To: Bhanu Pothugunta; Daniel J Cloutier
Cc: Anil Kumar Prathipati; Colleen McCormack
Subject: RE: Request to enable ports to generate TFA

Dan,

We are using the same proxy server as Raghu's team. we also included report server just in case in future if we need to use this AWS service as batch to send an emails/SMS. Please let me know if you have any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Bhanu Pothugunta
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Anil Kumar Prathipati <Anil.Prathipati@pcctg.com>; Keval Patel <Keval.Patel@pcctg.com>; Colleen McCormack <Colleen.McCormack@sos.nh.gov>
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,

Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Bhanu Pothugunta <bhanu.pothugunta@pcctg.com>
Sent: Tuesday, October 9, 2018 9:35 AM
To: Daniel J Cloutier
Cc: Anil Kumar Prathipati; Keval Patel; Colleen McCormack
Subject: Request to enable ports to generate TFA

Dan,

Can you open both 80 and 443 ports in below listed servers. Please let us know if you have any questions. Thank You.

URL: http://electionproxy.pcctg.net/
Public IP: 52.61.5.151
Ports:80 and 443

Servers:

IP ADDRESS	SERVER
10.12.20.102	OLD UAT
10.12.20.104	OLD APP SER 1 & 2 Multiple Instances
10.12.20.103	OLD RPT
10.144.27.24	New App server
10.144.27.27	New UAT server
10.144.27.25	New Production Report server
10.144.27.28	New UAT Report server

Regards,
Bhanu Pothugunta
O: 860.580.7687
M: 860.752.3834

Daniel J Cloutier

From: Colleen McCormack
Sent: Thursday, September 27, 2018 11:45 AM
To: Daniel J Cloutier; Anthony Stevens
Subject: 2FA Manual
Attachments: NH_TwoFactor_Authentication.docx

Thank You,

Colleen

Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Monday, September 24, 2018 12:16 PM
To: Colleen McCormack
Cc: Anthony Stevens; Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta; Sachin Shetty
Subject: Re: 2-Factor Authentication CCR 2018-002

Yes. I'll setup a call with you once we deploy. Also, we'll send release document. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

On Sep 24, 2018, at 12:12 PM, Colleen McCormack <Colleen.McCormack@sos.nh.gov> wrote:

> Keval
> We are good to go now to deploy 2FA in UAT.
> Will it take some walking through the process with me?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Monday, September 24, 2018 12:04 PM
To: Anthony Stevens
Cc: Colleen McCormack; Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta; Sachin Shetty
Subject: RE: 2-Factor Authentication CCR 2018-002

Anthony,

Good morning. We are ready to deploy 2FA for NH SVRS in UAT. Please let me know when do you want me to deploy it in UAT. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Friday, June 8, 2018 5:22 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: 2-Factor Authentication CCR 2018-002

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens
Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Colleen McCormack
Sent: Monday, September 24, 2018 12:13 PM
To: Keval Patel; Anthony Stevens
Cc: Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta; Sachin Shetty
Subject: RE: 2-Factor Authentication CCR 2018-002

Keval
We are good to go now to deploy 2FA in UAT.
Will it take some walking through the process with me?

Thank You,
Colleen
Colleen E. McCormack
HAVA
Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
NEW HAVA ADDRESS BELOW
HAVA Office at 9 Ratification Way, Concord, NH 03301
Phone: 800.540.5954 - Fax: 603.271.8242

From: Keval Patel [mailto:Keval.Patel@pcctg.com]
Sent: Monday, September 24, 2018 12:04 PM
To: Anthony Stevens
Cc: Colleen McCormack; Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta; Sachin Shetty
Subject: RE: 2-Factor Authentication CCR 2018-002

Anthony,

Good morning. We are ready to deploy 2FA for NH SVRS in UAT. Please let me know when do you want me to deploy it in UAT. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Friday, June 8, 2018 5:22 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: 2-Factor Authentication CCR 2018-002

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens
Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Monday, September 24, 2018 12:04 PM
To: Anthony Stevens
Cc: Colleen McCormack; Daniel J Cloutier; Anil Kumar Prathipati; Bhanu Pothugunta; Sachin Shetty
Subject: RE: 2-Factor Authentication CCR 2018-002

Anthony,

Good morning. We are ready to deploy 2FA for NH SVRS in UAT. Please let me know when do you want me to deploy it in UAT. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Director Product Support
Elections and Ethics Solutions
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
O. 860.466.7262 | C. 757.537.0781 | P. 860.242.3299

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Friday, June 8, 2018 5:22 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: 2-Factor Authentication CCR 2018-002

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens
Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Monday, June 11, 2018 10:39 AM
To: Anthony Stevens
Cc: Colleen McCormack; Daniel J Cloutier; Anand Balasubramanian
Subject: RE: 2-Factor Authentication CCR 2018-002
Attachments: CCR 2018-002 Final executed copy.pdf

Anthony,

Good Morning. Attached is the final executed copy of 2FA CR. I'll send you updated release plan for the 2FA. Let me know if any questions. Thank you.

With Regards,
Keval Patel | Program Manager
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Friday, June 8, 2018 5:22 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: 2-Factor Authentication CCR 2018-002

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens
Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Keval Patel <Keval.Patel@pcctg.com>
Sent: Friday, June 8, 2018 5:25 PM
To: Anthony Stevens
Cc: Colleen McCormack; Daniel J Cloutier; Anand Balasubramanian
Subject: RE: 2-Factor Authentication CCR 2018-002

Anthony,

Thanks for the approval. I'll send you final copy with Anand's signature.

With Regards,
Keval Patel | Program Manager
PCC Technology Inc., a GCR company | pcctg.com
100 Northfield Dr. Suite 300A | Windsor, CT 06095
P. 860.242.3299 | O. 860.466.7262 | C. 757.537.0781

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Friday, June 8, 2018 5:22 PM
To: Keval Patel <Keval.Patel@pcctg.com>
Cc: Colleen McCormack <Colleen.McCormack@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anand Balasubramanian <abalas@gcrincorporated.com>
Subject: 2-Factor Authentication CCR 2018-002

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens

Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Friday, June 8, 2018 5:22 PM
To: 'Keval Patel'
Cc: Colleen McCormack; Daniel J Cloutier; 'Anand Balasubramanian'
Subject: 2-Factor Authentication CCR 2018-002
Attachments: CCR 2018-002 Two-Factor Authentication.pdf

Keval,

Here is the signed CCR for Two-Factor Authentication.

You will note that I have changed the number to CCR 2018-002, since there already is a CCR 2018-001, signed on May 24, 2018.

Thanks for your help on this.

Anthony Stevens
Assistant Secretary of State
New Hampshire Department of State
Archives and Records Building
71 S. Fruit St.
Concord, New Hampshire 03301
Tel: (603)271-8238

Anomali Enterprise

Real-Time Forensics

Every day new threats are discovered, adding to the list of millions of known Indicators of Compromise (IOCs). This presents organizations with two challenges:

- Evaluating newly identified threats to identify an existing breach
- Checking millions of IOCs daily to identify newly launched attacks

The first challenge is especially critical. As new threats become known, organizations need to know if attackers have already targeted and breached their networks. This means being able to look over historical data going back 6 months or longer to identify potential breaches. The second challenge, checking millions of IOCs daily for new matches, addresses the need for organizations to maintain visibility into emerging threats to the network.

32% of organizations able to access data from **3 months ago**

4% of organizations are able to access data from **1 year ago**

2017 Ponemon Survey

Detecting New Threats

To determine if their organization was breached, security teams must take new threat intelligence and find any matches against recorded network activity over months or even years. Anomali developed the Real-Time Forensics (RTF) technology to complete searches over vast quantities of historical data in seconds instead of hours/days. RTF is the foundation of Anomali Enterprise, providing security teams instant visibility across all historical data.

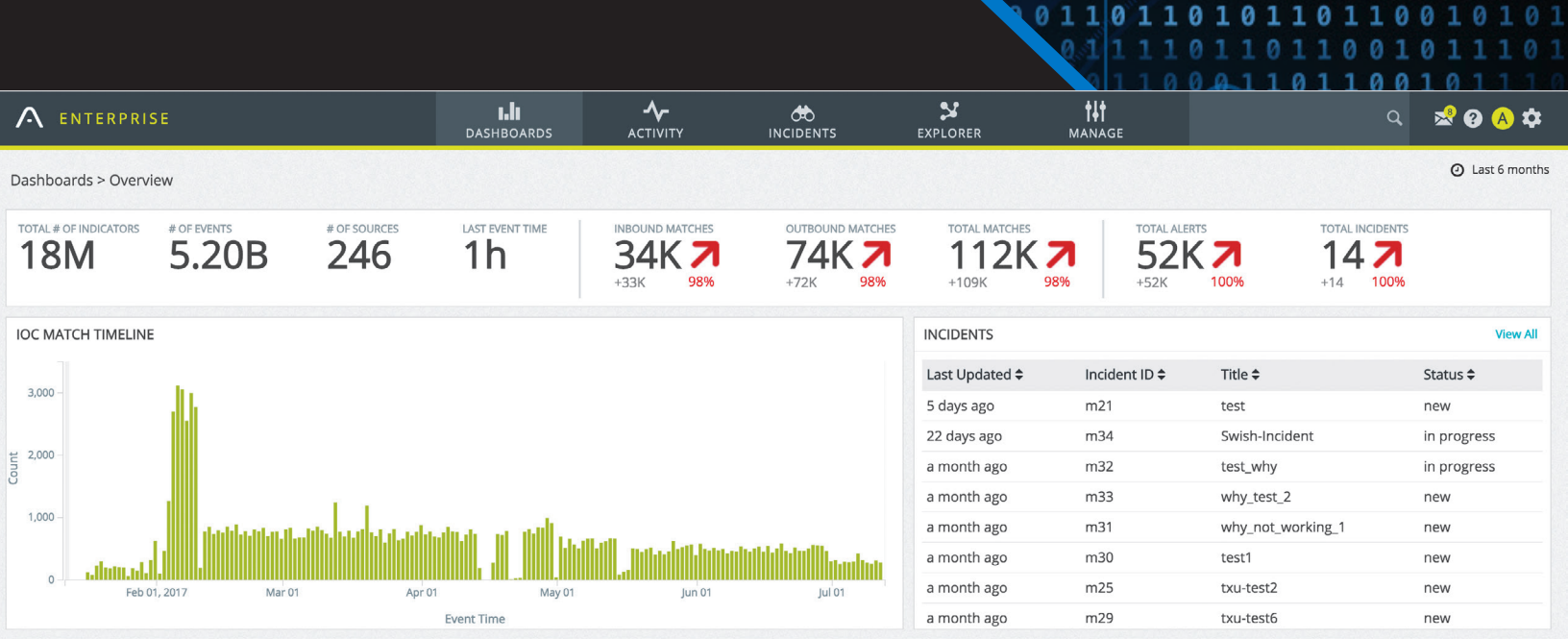
Detecting Existing Threats

Security teams are simultaneously charged with live monitoring their organization's health by comparing new traffic against known threats. Threat intelligence indicators can easily run into millions of indicators, each needing to be evaluated against internal log events. Anomali Enterprise is purpose-built to perform this massive scale intelligence matching, capable of processing millions of IOCs and billions of internal log entries. Positively identified "indicators of interest" are automatically fed to the SIEM for ongoing monitoring or blocking.

Indicators can also be enriched or added to investigations in ThreatStream, Anomali's Threat Intelligence Platform (TIP). Security teams can easily collaborate leveraging Anomali Enterprise's powerful search and scaling along with ThreatStream's integrations, sharing, and data enrichment.

Immediately identify threats with Real-Time Forensics

ANOMALI®
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com



Intuitive interface and dashboards reveal threat matches, streamlines analysis

Core Capabilities

Anomali Enterprise integrates with your existing SIEM and other log sources, maintaining a year or more of historical visibility without duplicating logs. This historical data is continuously correlated against new and existing threat intelligence to uncover evidence of breaches. Real-Time Forensics immediately discovers matches between these data sets, reducing time to detection to a matter of seconds. Anomali Enterprise also provides analysts with tools to categorize and elevate indicator matches for triage and response.

- Quickly identifies newly discovered threats against 365+ days historical data
- Matches billions of daily network events against millions of IOCs in seconds
- Detects malicious activity with DGA algorithms
- Delivers high priority IOCs to SIEMs for ongoing monitoring

DGA

Domain Generation Algorithms are widely used in malware to set up command and control domains. The malware is instructed to phone home to DGA-produced domain names. These domains often live for a day or two and tend to have nonsensical names - e.g., jcxeionotdssqkdun.pw. Given their short lifespans, DGA domains do not make it onto threat intelligence lists. Nevertheless, Anomali Enterprise is able to detect and alert on traffic to DGA domains. The solution discovers DGA activity using sophisticated algorithms and does not rely on documented threat indicators.

Get the Ponemon study:
State of Threat Intelligence:
anomali.com/ponemon

Event Time	Event Source	Destination	URL	DGA Probability	Malware Family	Count
Aug 30th 2017, 19:50:00 -05:00	172.18.15.16	wgtbnpt64a74r7wdnyoygsqpz8s.com	-	0.96	Gameover_DGA, MadMax	11
Aug 30th 2017, 19:50:00 -05:00	172.18.19.14	tjotvtrdd1jdb9hd6xb4o85icf.com	-	1	Gameover_DGA, MadMax	16
Aug 30th 2017, 19:50:00 -05:00	172.18.13.15	1pdhc2u20gf32oqunv8uqpzbgc6.com	-	0.99	Gameover_DGA, MadMax	6
Aug 30th 2017, 19:50:00 -05:00	172.18.20.13	gh8eoyfrvr0ayxxt.com	-	0.903	Bedep, Chinad, Corebot, MadMax	8

Anomali Enterprise has powerful DGA detection capabilities

ANOMALI®
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com

Domain Monitoring Service

Challenge

Defenders face numerous challenges trying to protect organizations from cyber attacks. Many of the tools available take a reactive approach to threats, leaving organizations to wait for attacks and hope that their defenses will detect or stop them. Monitoring domain registrations is one way to proactively detect when criminals stand up infrastructure to be used in a future attack.

Attackers frequently attempt to bypass existing security controls by registering domains that mimic authentic corporate infrastructure. These domains can be weaponized within hours of registration and subsequently used for delivery of malicious payloads and exfiltration of sensitive data. The ability to detect these malicious domains within one hour of registration is therefore essential to a proactive security posture.

The Anomali Domain Monitoring Service is a yearly subscription that includes monitoring a customized number of domains or keywords for new suspicious registrations. This service enables security teams to:

- Detect attacker infrastructure before it is used;
- Disrupt an attacker's ability to create an outbound channel (e.g command and control);
- Prevent harvesting and exfiltration of data.

How It Works

The Anomali proprietary algorithm identifies homoglyphs — characters that appears very much like another (e.g. number 0 and uppercase O) — and look-alike domains and converts them to IOCs in ThreatStream within one to four hours of generic top-level domain (gTLD) registration. Seasoned security analysts and threat researchers also manually review and report (within 48 hours) any additional anomalous activity associated with registrations.

Identified domains are imported into ThreatStream and customer integrations, automatically providing clients with:

- Alerts of newly registered domains;
- Details of newly registered domains as Threat Bulletins;
- New potential Indicators of Compromise (IOCs) for further investigation.

The Domain Monitoring Service also detects and reviews domains that may be in violation of corporate brand infringement.

Use Cases

Homoglpyhic and look-alike domains play an integral role in various parts of the Cyber Kill Chain. For the example of companyX.com, a malicious actor may register the domain c0mpanyX.com. This domain can then be weaponized and subsequently used in one to all of the following common attack vectors:

1. **Phishing attack** (Delivery part of the Kill Chain). An email is sent to an employee attempting to entice them to send their credentials to dropbox.c0mpanyX.com.
2. **Command and Control** (Command and Control part of the Kill Chain). Attacker configures their backdoor or malware to communicate to c0mpanyX.com for further instructions.
3. **Exfiltration** ("Actions on Objective" part of the Kill Chain). Attacker sends stolen data back to c0mpanyX.com. This homoglyphic domain may be

missed by companyX.com's security team.

The following attack timelines outline the sequence of events for a Phishing attack with and without the Domain Monitoring Service. In both cases, the attacker is successful in tricking an employee to reveal their credentials. The idea being that, even with a very effective phishing awareness program, given enough phishing attempts — some will be delivered and eventually someone will click. With the Domain Monitoring Service, companyX.com is able to intervene and prevent any critical damage.

Attack Timeline for Phishing Use Case		Attack Timeline with Domain Monitoring Service
Actor registers **c0mpanyX.com**	00:00	Actor registers **c0mpanyX.com**
	00:45	c0mpanyX.com is identified as a **suspicious domain** and imported into ThreatStream. SOC personnel from companyX.com are alerted.
Attacker successfully **delivers phishing email** to companyX.com	01:00	Attacker successfully **delivers phishing email** to targeted company
	01:30	companyX.com SOC deems c0mpanyX.com domain to be suspicious and **blocks all outbound connections** to c0mpanyX.com
Employee at companyX.com is duped by email and **sends their credentials** to the attacker	02:00	Employee at companyX.com is duped by the email and sends their credentials to the attacker, but **the connection is blocked.**
Attacker enters network with employee credentials and **attempts to establish persistence**	03:00	

For additional information or to schedule a consultation please contact
cso-ps@anomali.com

Corporate office: 808 Winslow Street, Redwood City, CA 94063

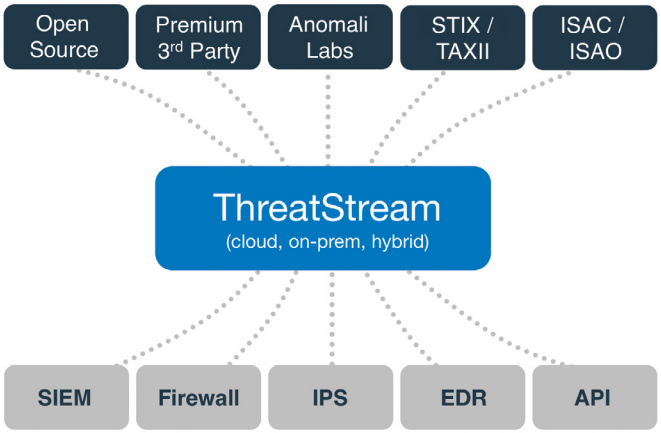
ANOMALI®

ThreatStream®

The Most Widely Adopted Threat Intelligence Platform

Threat Intelligence Overload

SOC analysts, incident response teams and researchers face the challenge of operationalizing an overwhelming amount of threat data. A recent Ponemon survey showed that 78% say threat intelligence is critical for achieving a strong security posture but also showed that 70% are overwhelmed with threat data. Anomali ThreatStream® makes it easier for security teams to achieve the full promise of threat intelligence. ThreatStream automates all the processes for collecting, managing and integrating threat intelligence, and gives security analysts the tools and resources to respond quickly to active threats.



Get the Ponemon study:
State of Threat Intelligence:
anomali.com/ponemon

Collect

ThreatStream manages ingesting intelligence from many disparate sources, including:

- STIX/TAXII feeds
- Open source threat feeds
- Commercial threat intelligence providers
- Unstructured intelligence: PDFs, CSVs, emails
- ISAC/ISAO shared threat intelligence

Manage

ThreatStream takes raw threat data and turns it into rich, usable intelligence:

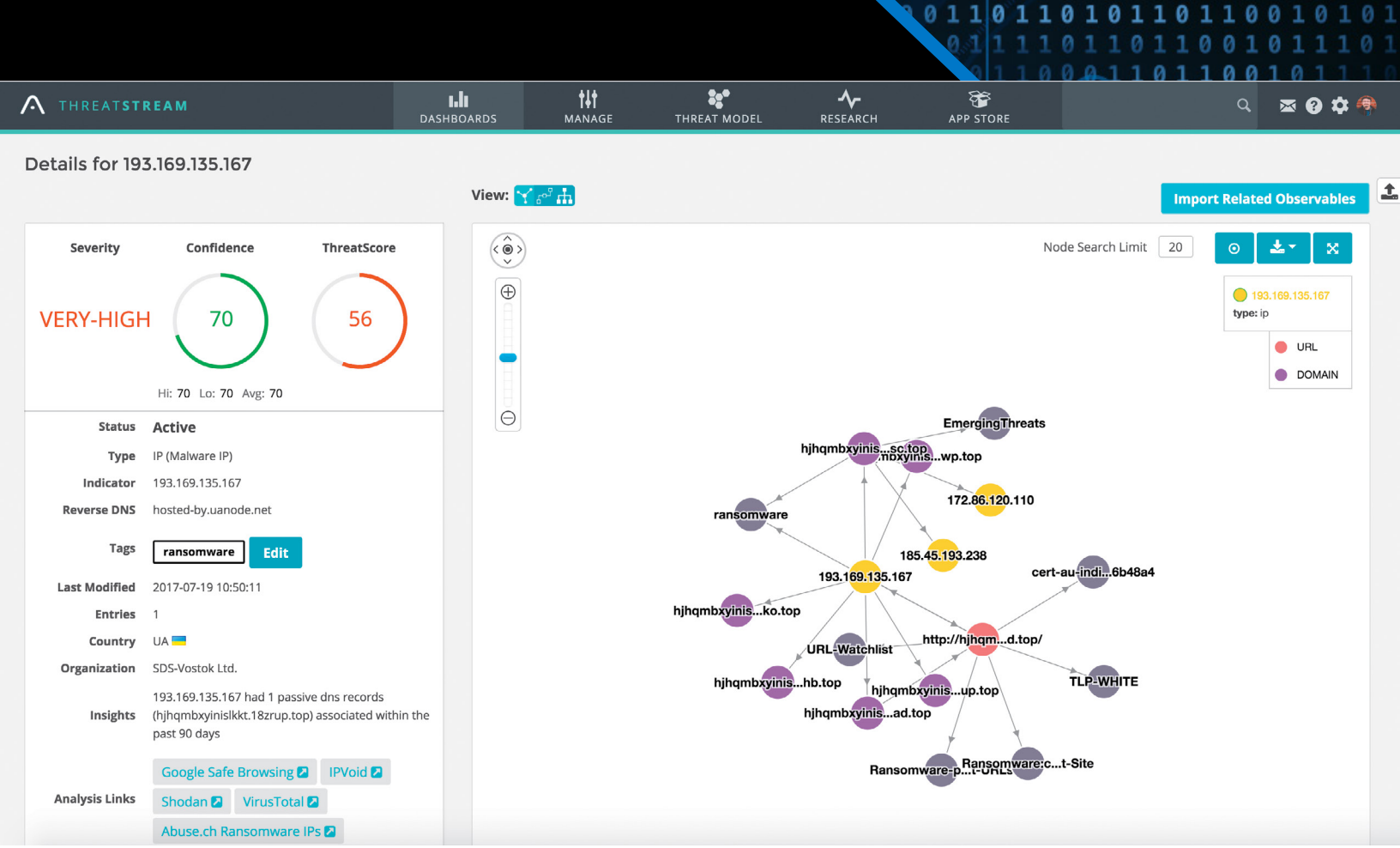
- Normalizes feeds into a common taxonomy
- De-duplicates data across feeds
- Removes false positives
- Enriches data with actor, campaign, and TTP
- Associates related threat indicators

Integrate

ThreatStream integrates with internal security systems to make threat intelligence actionable.

- Deep integration with SIEM, FW, IPS, and EDR
- Scales to process millions of indicators
- Risk ranks threats via machine learning
- Includes Threat Bulletins from Anomali Labs
- Secure, 2-way sharing with Trusted Circles

808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com



Enabling the Analyst

Anomali ThreatStream provides tools to make analysts more efficient and increase the effectiveness of their use of threat intelligence. The ThreatStream platform includes analyst-friendly features such as:

- Malicious file examination via a built-in sandbox
- Association of indicators to cyber Actors
- Contextual data: WHOIS, PassiveDNS, others
- Threat investigation engine with analyst workflows
- Easily produce and share threat intelligence
- Brand monitoring: detection of brand abuse
- Collaborate with peers via Trusted Circles

ThreatStream Advantages

ThreatStream speeds detection and response time by operationalizing threat intelligence and uniting your security tools under one platform.

- Centralizes all your threat intel data in one place
- Turns raw indicators into actionable intelligence
- Integrates with existing security investments
- Accelerates incident response time
- Makes security analysts more efficient

To find out more about Anomali ThreatStream visit www.anomali.com/threatstream or contact info@anomali.com.

ANOMALI®
808 Winslow Street, Redwood City, CA 94063 USA
1-844-4-THREATS | info@anomali.com | www.anomali.com

Daniel J Cloutier

From: Orville Fitch
Sent: Thursday, May 30, 2019 8:17 AM
To: Daniel J Cloutier
Subject: RE: Checking back

Dan,
That was my understanding as well. I do wonder if what they are proposing is a third party that would use their information and produce something more like what we are able to consume. I yield to your judgment on a response. I think in the sales world there are sometimes metrics that motivate sales people to keep prospective clients alive and drive up the number of contacts even when a sale will not occur. Maybe that is what is going on.
Bud

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Wednesday, May 29, 2019 12:00 PM
To: Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: Checking back

Bud,

I thought we ruled out Anomali as a possible vendor to provide web monitoring information?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: James Orrange <jorrange@anomali.com>
Sent: Wednesday, May 29, 2019 10:19 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Thomas Oppel <tpoppel@mabusgroup.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

A quick update from our last call.
I have made contact with one of our partners that provide Anomali as a hosted turnkey service.
Once I have confirmed some open times with them I will get back to everyone with some options.

jo

On Mon, May 6, 2019 at 4:05 PM Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier

Assistant Secretary of State

New Hampshire Department of State

Information Technology Office

NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier

Assistant Secretary of State

New Hampshire Department of State

Information Technology Office

NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

--
Regards,

James Orrange
Anomali
281.932.3047

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Wednesday, May 29, 2019 12:00 PM
To: Orville Fitch
Subject: Checking back

Bud,

I thought we ruled out Anomali as a possible vendor to provide web monitoring information?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: James Orrange <jorrange@anomali.com>
Sent: Wednesday, May 29, 2019 10:19 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Thomas Oppel <tpoppel@mabusgroup.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

A quick update from our last call.
I have made contact with one of our partners that provide Anomali as a hosted turnkey service.
Once I have confirmed some open times with them I will get back to everyone with some options.

jo

On Mon, May 6, 2019 at 4:05 PM Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier

Assistant Secretary of State

New Hampshire Department of State

Information Technology Office

NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier

Assistant Secretary of State

New Hampshire Department of State

Information Technology Office

NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger

<meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

--
Regards,

James Orrange
Anomali
281.932.3047

Daniel J Cloutier

From: James Orrange <jorrange@anomali.com>
Sent: Wednesday, May 29, 2019 10:19 AM
To: Daniel J Cloutier
Cc: Thomas Oppel; John Kitchen; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

A quick update from our last call.
I have made contact with one of our partners that provide Anomali as a hosted turnkey service.
Once I have confirmed some open times with them I will get back to everyone with some options.

jo

On Mon, May 6, 2019 at 4:05 PM Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.
>
> Thanks,
>
> *Dan*
>
> Daniel J Cloutier
>
> Assistant Secretary of State
>
> New Hampshire Department of State
>
> Information Technology Office
>
> NH State Archives - Room 209
>
> 9 Ratification Way, Concord, NH 03301
>
> Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier

Assistant Secretary of State

New Hampshire Department of State

Information Technology Office

NH State Archives - Room 209

9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

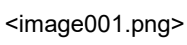
From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)



--
Regards,

James Orrange
Anomali
281.932.3047

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 12:00 PM
To: Daniel J Cloutier
Cc: Orville Fitch; Anthony Stevens; John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Great, Dan. Thanks

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On May 7, 2019, at 11:40, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Both are Assistant Secretaries of State as I am; Bud is our Elections Attorney (former NH Deputy Attorney General) and Anthony is our Elections Director.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
Director of IT
Data Security Officer

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:40 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Orville Fitch <Orville.Fitch@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Do Mr. Fitche and Stevens work with you or another agency?

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 09:39, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

It will only be the other two I added to the email stream (Fitch & Stevens). If I can get others I will invite them separately.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:38 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>

Cc: Orville Fitch <Orville.Fitch@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

That's great! Thanks so much. We'll be ready to go with call in info shortly. Please let us know who else from NH will be on the call when you can.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 09:36, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

We are a GO for today, May 7, 2019, 2PM EDST. Please send us a meeting request with the appropriate connection requirements.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson

<jferguson@anomali.com>
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> ---
>
> **From:** Thomas Oppel <tpoppel@mabusgroup.com>
> **Sent:** Tuesday, April 23, 2019 11:20 AM
> **To:** Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>

Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is

not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire
Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way,
Concord, NH 03301
Phone: 603.271.0001 -
Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, May 7, 2019 11:41 AM
To: 'Thomas Oppel'
Cc: Orville Fitch; Anthony Stevens; John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: RE: Checking back

Both are Assistant Secretaries of State as I am; Bud is our Elections Attorney (former NH Deputy Attorney General) and Anthony is our Elections Director.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
Director of IT
Data Security Officer

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:40 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Orville Fitch <Orville.Fitch@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Do Mr. Fitche and Stevens work with you or another agency?

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On May 7, 2019, at 09:39, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

It will only be the other two I added to the email stream (Fitch & Stevens). If I can get others I will invite them separately.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

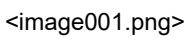
From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:38 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Orville Fitch <Orville.Fitch@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

That's great! Thanks so much. We'll be ready to go with call in info shortly. Please let us know who else from NH will be on the call when you can.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)



On May 7, 2019, at 09:36, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

We are a GO for today, May 7, 2019, 2PM EDST. Please send us a meeting request with the appropriate connection requirements.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of

these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group

1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:40 AM
To: Daniel J Cloutier
Cc: Orville Fitch; Anthony Stevens; John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Roger. Do Mr. Fitche and Stevens work with you or another agency?

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On May 7, 2019, at 09:39, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

It will only be the other two I added to the email stream (Fitch & Stevens). If I can get others I will invite them separately.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:38 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Orville Fitch <Orville.Fitch@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

That's great! Thanks so much. We'll be ready to go with call in info shortly. Please let us know who else from NH will be on the call when you can.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 09:36, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

We are a GO for today, May 7, 2019, 2PM EDST. Please send us a meeting request with the appropriate connection requirements.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B

Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)

(603) 304-6767 (C)

<image002.png>

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>;

Meredith Berger
<meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, May 7, 2019 9:45 AM
To: jkitchen@anomali.com
Subject: Accepted: Invitation: NH SOS/Mabus/Anomali Demonstration @ Tue May 7, 2019 2pm - 3pm (EDT) (daniel.cloutier@sos.nh.gov)

Daniel J Cloutier

Subject: Invitation: NH SOS/Mabus/Anomali Demonstration @ Tue May 7, 2019 2pm - 3pm (EDT) (daniel.cloutier@sos.nh.gov)
Location: https://anomali.zoom.us/j/132254203

Start: Tue 5/7/2019 2:00 PM
End: Tue 5/7/2019 3:00 PM

Recurrence: (none)

Meeting Status: Accepted

Organizer: jkitchen@anomali.com

You have been invited to the following event.

more details »

NH SOS/Mabus/Anomali Demonstration

When Tue May 7, 2019 2pm – 3pm Eastern Time - New York

Where https://anomali.zoom.us/j/132254203 (map)

Calendar daniel.cloutier@sos.nh.gov

Who
- jkitchen@anomali.com - organizer
- tpoppel@mabusgroup.com
- daniel.cloutier@sos.nh.gov
- meredith@mabusgroup.com
- jorrange@anomali.com
- anthony.stevens@sos.nh.gov
- jferguson@anomali.com
- orville.fitch@sos.nh.gov

John Kitchen is inviting you to a scheduled Zoom meeting.

Join Zoom Meeting

https://anomali.zoom.us/j/132254203

One tap mobile

+16465588656,,132254203# US (New York)

+16699006833,,132254203# US (San Jose)

Dial by your location

+1 646 558 8656 US (New York)

+1 669 900 6833 US (San Jose)

Meeting ID: 132 254 203

Find your local number: https://zoom.us/u/aWKpdkKta

Join by SIP

132254203@zoomcrc.com

Join by H.323

162.255.37.11 (US West)

162.255.36.11 (US East)

221.122.88.195 (China)

115.114.131.7 (India)

213.19.144.110 (EMEA)

202.177.207.158 (Australia)

209.9.211.110 (Hong Kong)

64.211.144.160 (Brazil)

69.174.57.160 (Canada)

Meeting ID: 132 254 203

Going (daniel.cloutier@sos.nh.gov)? **Yes** - **Maybe** - **No** more options »

Invitation from Google Calendar

You are receiving this courtesy email at the account daniel.cloutier@sos.nh.gov because you are an attendee of this event.

To stop receiving future updates for this event, decline this event. Alternatively you can sign up for a Google account at https://www.google.com/calendar/ and control your notification settings for your entire calendar.

Forwarding this invitation could allow any recipient to send a response to the organizer and be added to the guest list, or invite others regardless of their own invitation status, or to modify your RSVP. Learn More.

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, May 7, 2019 9:39 AM
To: 'Thomas Oppel'
Cc: Orville Fitch; Anthony Stevens; John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: RE: Checking back

Tracking:

Recipient	Read
'Thomas Oppel'	
Orville Fitch	Read: 5/7/2019 9:41 AM
Anthony Stevens	Read: 5/7/2019 10:02 AM
John Kitchen	
James Orrange	
Meredith Berger	
Jason Ferguson	

It will only be the other two I added to the email stream (Fitch & Stevens). If I can get others I will invite them separately.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:38 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: Orville Fitch <Orville.Fitch@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

That's great! Thanks so much. We'll be ready to go with call in info shortly. Please let us know who else from NH will be on the call when you can.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On May 7, 2019, at 09:36, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

We are a GO for today, May 7, 2019, 2PM EDST. Please send us a meeting request with the appropriate connection requirements.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me

know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

> On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:
>
> Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 9:38 AM
To: Daniel J Cloutier
Cc: Orville Fitch; Anthony Stevens; John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Dan

That's great! Thanks so much. We'll be ready to go with call in info shortly. Please let us know who else from NH will be on the call when you can.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On May 7, 2019, at 09:36, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

We are a GO for today, May 7, 2019, 2PM EDST. Please send us a meeting request with the appropriate connection requirements.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>

Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> ---
>
> **From:** Thomas Oppel <tpoppel@mabusgroup.com>
> **Sent:** Tuesday, April 23, 2019 11:20 AM
> **To:** Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
> **Cc:** John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
> **Subject:** Re: Checking back
>
> Dan
>
> Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.
>
> Thomas P. Oppel
>
> The Mabus Group
> 1700 K Street, NW

Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

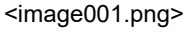
From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)



Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, May 7, 2019 9:36 AM
To: 'Thomas Oppel'; Orville Fitch; Anthony Stevens
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: RE: Checking back

Tracking:

Recipient	Read
'Thomas Oppel'	
Orville Fitch	Read: 5/7/2019 9:37 AM
Anthony Stevens	
John Kitchen	
James Orrange	
Meredith Berger	
Jason Ferguson	

We are a GO for today, May 7, 2019, 2PM EDST. Please send us a meeting request with the appropriate connection requirements.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)

MABUS GROUP

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as

another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

> On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:
>
> Hi Thomas,
>
> Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that

next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, May 7, 2019 8:35 AM
To: Daniel J Cloutier
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Roger. Standing by

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On May 7, 2019, at 08:11, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger

<meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> ---
>
> **From:** Thomas Oppel <tpoppel@mabusgroup.com>
> **Sent:** Tuesday, April 23, 2019 11:20 AM
> **To:** Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
> **Cc:** John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
> **Subject:** Re: Checking back
>
> Dan
>
> Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.
>
> Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

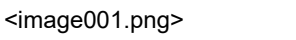
From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)



Daniel J Cloutier

From: Orville Fitch
Sent: Tuesday, May 7, 2019 8:48 AM
To: Daniel J Cloutier
Subject: RE: Checking back

Yes

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Tuesday, May 07, 2019 8:10 AM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: RE: Checking back

Can you two be available for a 2PM virtual presentation that would last an hour but no longer than 2 hours?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Tuesday, April 30, 2019 3:51 PM
To: Orville Fitch <Orville.Fitch@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: Checking back

Dan,

Monday, 6th and Tuesday, 7th are open.
Wed, 8th: Clerk's Regional Workshop
Thurs, 9th: Appointment at 3 PM
Fri., 10th: Looks open for now

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Orville Fitch <Orville.Fitch@sos.nh.gov>
Sent: Tuesday, April 30, 2019 8:10 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: RE: Checking back

Dan,
Monday 6th and Tuesday 7th are open.
Wed Clerk's Regional
Thurs 15-A meeting with Pcc
Friday – on hold for AWS

Bud

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Monday, April 29, 2019 7:10 PM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: Checking back

Anthony & Bud,

This is the company I just emailed you about. They have an alternative to the GroupSense/FireEye web alert system. What does your next week look like now?

Dan

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, May 7, 2019 8:12 AM
To: 'Thomas Oppel'
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Checking back

Thomas,

I am checking with staff. It is more likely than not that a 2PM presentation will work but I won't know for sure until around 9AM.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever

books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

> On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:
>
> Hi Thomas,
>
> Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, May 7, 2019 8:10 AM
To: Anthony Stevens; Orville Fitch
Subject: RE: Checking back

Tracking:

Recipient	Read
Anthony Stevens	Read: 5/7/2019 10:00 AM
Orville Fitch	Read: 5/7/2019 8:47 AM

Can you two be available for a 2PM virtual presentation that would last an hour but no longer than 2 hours?

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Tuesday, April 30, 2019 3:51 PM
To: Orville Fitch <Orville.Fitch@sos.nh.gov>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: RE: Checking back

Dan,

Monday, 6th and Tuesday, 7th are open.
Wed, 8th: Clerk's Regional Workshop
Thurs, 9th: Appointment at 3 PM
Fri., 10th: Looks open for now

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Orville Fitch <Orville.Fitch@sos.nh.gov>
Sent: Tuesday, April 30, 2019 8:10 AM

To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: RE: Checking back

Dan,
Monday 6th and Tuesday 7th are open.
Wed Clerk's Regional
Thurs 15-A meeting with Pcc
Friday – on hold for AWS

Bud

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Monday, April 29, 2019 7:10 PM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: Checking back

Anthony & Bud,

This is the company I just emailed you about. They have an alternative to the GroupSense/FireEye web alert system. What does your next week look like now?

Dan

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Monday, May 6, 2019 5:11 PM
To: Daniel J Cloutier
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Dan

I think everyone could still do a virtual presentation tomorrow after 2. I have a another call at 4 so I'd need to be done by then.

Sent from my iPhone

On May 6, 2019, at 16:04, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.
>
> Thanks,
> *Dan*
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> ---
>
> **From:** Thomas Oppel <tpoppel@mabusgroup.com>
> **Sent:** Tuesday, April 23, 2019 11:20 AM
> **To:** Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
> **Cc:** John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
> **Subject:** Re: Checking back
>
> Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image002.png>

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

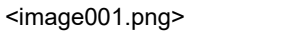
From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)



Daniel J Cloutier

From: Daniel J Cloutier
Sent: Monday, May 6, 2019 4:04 PM
To: 'Thomas Oppel'
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: RE: Checking back

Thomas,

As I was in Denver last week, it does not look like I finished sending you our schedules for this week. Everyone was available for tomorrow, Tuesday, May 7th (but that is unlikely for you now.) Wednesday and Thursday are out. Friday is a big maybe as another meeting may take place but is not yet scheduled so whomever books it first may just get the nod. Let me know if any of these dates work otherwise we can shoot for next week or so.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Anthony Stevens
Sent: Tuesday, April 30, 2019 3:51 PM
To: Orville Fitch; Daniel J Cloutier
Subject: RE: Checking back

Dan,

Monday, 6th and Tuesday, 7th are open.
Wed, 8th: Clerk's Regional Workshop
Thurs, 9th: Appointment at 3 PM
Fri., 10th: Looks open for now

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Orville Fitch <Orville.Fitch@sos.nh.gov>
Sent: Tuesday, April 30, 2019 8:10 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Subject: RE: Checking back

Dan,
Monday 6th and Tuesday 7th are open.
Wed Clerk's Regional
Thurs 15-A meeting with Pcc
Friday – on hold for AWS

Bud

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Monday, April 29, 2019 7:10 PM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: Checking back

Anthony & Bud,

This is the company I just emailed you about. They have an alternative to the GroupSense/FireEye web alert system. What does your next week look like now?

Dan

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>

Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Orville Fitch
Sent: Tuesday, April 30, 2019 8:10 AM
To: Daniel J Cloutier; Anthony Stevens
Subject: RE: Checking back

Dan,
Monday 6th and Tuesday 7th are open.
Wed Clerk's Regional
Thurs 15-A meeting with Pcc
Friday – on hold for AWS

Bud

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Monday, April 29, 2019 7:10 PM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: Checking back

Anthony & Bud,

This is the company I just emailed you about. They have an alternative to the GroupSense/FireEye web alert system. What does your next week look like now?

Dan

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Monday, April 29, 2019 7:10 PM
To: Anthony Stevens; Orville Fitch
Subject: Checking back

Tracking:

Recipient	Read
Anthony Stevens	
Orville Fitch	Read: 4/30/2019 8:08 AM

Anthony & Bud,

This is the company I just emailed you about. They have an alternative to the GroupSense/FireEye web alert system. What does your next week look like now?

Dan

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Jason Ferguson <jferguson@anomali.com>
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, April 23, 2019 11:20 AM
To: Daniel J Cloutier
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Dan

Looks like our team is pretty open the week of May 6, so check with your folks and shoot me some times that week that work for everyone in NH.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Friday, April 19, 2019 12:30 PM
To: Daniel J Cloutier
Cc: John Kitchen; James Orrange; Meredith Berger; Jason Ferguson
Subject: Re: Checking back

Dan

Thanks so much for getting back. I figured with Legislature in session that alone would keep you hopping! Let me talk to the folks at Anomali and get back to you on dates, but sounds like sometime in May.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

On Apr 19, 2019, at 12:13, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Friday, April 19, 2019 12:14 PM
To: 'Thomas Oppel'
Cc: John Kitchen; James Orrange; Meredith Berger
Subject: Checking back

Hi Thomas,

Yes, it has been busy. What dates/times were you looking for us to view? At the moment I do know that next week is not good for Deputy Scanlan and I am away the following week. So it can be as early as the week of May 6th. Let me know and I will check with Dave and other staff who could benefit from your services.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: John Kitchen <jkitchen@anomali.com>; James Orrange <jorrange@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Wednesday, March 27, 2019 3:56 PM
To: Daniel J Cloutier
Cc: John Kitchen; James Orrange; Meredith Berger
Subject: Checking back

Dan

I'm sure you've been swamped, but wanted to check in to see if we might set up an online demo of Anomali for you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

MABUS GROUP

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Thursday, March 7, 2019 12:03 PM
To: Daniel J Cloutier
Cc: James Orrange; John Kitchen; Meredith Berger
Subject: Re: Confirming

Will do sir. Didn't want to pester but did want to make sure you had received. Have a great weekend.

Sent from my iPhone

> On Mar 7, 2019, at 11:18, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:
>
> I have received the information and working in a time to ingest. Ping me back next week if you do not hear back from me please.
>
> Thanks,
> Dan
> Daniel J Cloutier
> Assistant Secretary of State
> New Hampshire Department of State
>
> Information Technology Office
> NH State Archives - Room 209
> 9 Ratification Way, Concord, NH 03301
> Phone: 603.271.0001 - Fax: 603.271.8242
>
> -----Original Message-----
> From: Thomas Oppel <tpoppel@mabusgroup.com>
> Sent: Thursday, March 7, 2019 9:39 AM
> To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
> Cc: James Orrange <jorrange@anomali.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
> Subject: Confirming
>
> Dan
>
> Just making sure you got the attachments and if you have any further questions or info requests.
>
> Sent from my iPhone

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, March 7, 2019 11:18 AM
To: 'Thomas Oppel'
Cc: James Orrange; John Kitchen; Meredith Berger
Subject: RE: Confirming

I have received the information and working in a time to ingest. Ping me back next week if you do not hear back from me please.

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

-----Original Message-----
From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Thursday, March 7, 2019 9:39 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: James Orrange <jorrange@anomali.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>
Subject: Confirming

Dan

Just making sure you got the attachments and if you have any further questions or info requests.

Sent from my iPhone

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Thursday, March 7, 2019 9:39 AM
To: Daniel J Cloutier
Cc: James Orrange; John Kitchen; Meredith Berger
Subject: Confirming

Dan

Just making sure you got the attachments and if you have any further questions or info requests.

Sent from my iPhone

Daniel J Cloutier

From: James Orrange <jorrange@anomali.com>
Sent: Tuesday, March 5, 2019 4:40 PM
To: Daniel J Cloutier
Cc: Thomas Oppel; William Gardner; David Scanlan
Subject: Re: Thank you!
Attachments: Anomali_Enterprise_Data_Sheet.pdf; Anomali-Domain-Monitoring-Service.pdf; ThreatStream-Datasheet (1).pdf

Dan,

Attached are a couple informational Data Sheets about Anomali.
Please let me know if I can assist further.

James
281.932.3047

On Tue, Mar 5, 2019 at 12:19 PM Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

> Thomas,
>
> I will check with Dan Dister, state CISO to see if he is interested but in the meantime, I await some information about Anomali from you, Jim, or John that I can peruse prior to our next meeting.
>
> Thanks,
>
> *Dan*
>
> Daniel J Cloutier
>
> Assistant Secretary of State
>
> New Hampshire Department of State
>
> Information Technology Office
>
> NH State Archives - Room 209
>
> 9 Ratification Way, Concord, NH 03301

Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Saturday, March 2, 2019 12:22 PM
To: William Gardner <wgardner@sos.nh.gov>; David Scanlan <David.Scanlan@SOS.NH.GOV>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: James Orrange <jorrange@anomali.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Paula Penney <Paula.Penney@SOS.NH.GOV>
Subject: Thank you!

Secretary Gardner, Deputy Secretary Scanlan and Assistant Secretary Cloutier

Thank you again for your willingness to meet with us and to connect us with Dan to discuss the capabilities of Anomali. John Kitchen, James Orrange and I hope you thought the meetings were as productive as we believe they were.

As we discussed, we'd like to set up a time to provide an online WebEx session to demonstrate Anomali more in depth. Can you provide a couple of dates and times this month that would work best for you? We'd also like to see if Commissioner Goulet and Director Plummer might wish to participate.

Again, thanks for your time and look forward to talking again soon.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

--
Regards,

James Orrange
Anomali
281.932.3047

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Tuesday, March 5, 2019 12:22 PM
To: Daniel J Cloutier
Cc: William Gardner; David Scanlan; James Orrange; John Kitchen; Meredith Berger; Paula Penney
Subject: Re: Thank you!

Yes, sir. We'll get it to you today.

Thank you.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

On Mar 5, 2019, at 12:18, Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov> wrote:

Thomas,

I will check with Dan Dister, state CISO to see if he is interested but in the meantime, I await some information about Anomali from you, Jim, or John that I can peruse prior to our next meeting.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Saturday, March 2, 2019 12:22 PM
To: William Gardner <wgardner@sos.nh.gov>; David Scanlan <David.Scanlan@SOS.NH.GOV>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: James Orrange <jorrange@anomali.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Paula Penney <Paula.Penney@SOS.NH.GOV>
Subject: Thank you!

Secretary Gardner, Deputy Secretary Scanlan and Assistant Secretary Cloutier

Thank you again for your willingness to meet with us and to connect us with Dan to discuss the capabilities of Anomali. John Kitchen, James Orrange and I hope you thought the meetings were as productive as we believe they were.

As we discussed, we'd like to set up a time to provide an online WebEx session to demonstrate Anomali more in depth. Can you provide a couple of dates and times this month that would work best for you? We'd also like to see if Commissioner Goulet and Director Plummer might wish to participate.

Again, thanks for your time and look forward to talking again soon.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

<image001.png>

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Tuesday, March 5, 2019 12:18 PM
To: 'Thomas Oppel'; William Gardner; David Scanlan
Cc: James Orrange; John Kitchen; Meredith Berger; Paula Penney
Subject: Thank you!

Thomas,

I will check with Dan Dister, state CISO to see if he is interested but in the meantime, I await some information about Anomali from you, Jim, or John that I can peruse prior to our next meeting.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Saturday, March 2, 2019 12:22 PM
To: William Gardner <wgardner@sos.nh.gov>; David Scanlan <David.Scanlan@SOS.NH.GOV>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: James Orrange <jorrange@anomali.com>; John Kitchen <jkitchen@anomali.com>; Meredith Berger <meredith@mabusgroup.com>; Paula Penney <Paula.Penney@SOS.NH.GOV>
Subject: Thank you!

Secretary Gardner, Deputy Secretary Scanlan and Assistant Secretary Cloutier

Thank you again for your willingness to meet with us and to connect us with Dan to discuss the capabilities of Anomali. John Kitchen, James Orrange and I hope you thought the meetings were as productive as we believe they were.

As we discussed, we'd like to set up a time to provide an online WebEx session to demonstrate Anomali more in depth. Can you provide a couple of dates and times this month that would work best for you? We'd also like to see if Commissioner Goulet and Director Plummer might wish to participate.

Again, thanks for your time and look forward to talking again soon.

Thomas P. Oppel

The Mabus Group

1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

Daniel J Cloutier

From: Thomas Oppel <tpoppel@mabusgroup.com>
Sent: Saturday, March 2, 2019 12:22 PM
To: William Gardner; David Scanlan; Daniel J Cloutier
Cc: James Orrange; John Kitchen; Meredith Berger; Paula Penney
Subject: Thank you!

Secretary Gardner, Deputy Secretary Scanlan and Assistant Secretary Cloutier

Thank you again for your willingness to meet with us and to connect us with Dan to discuss the capabilities of Anomali. John Kitchen, James Orrange and I hope you thought the meetings were as productive as we believe they were.

As we discussed, we'd like to set up a time to provide an online WebEx session to demonstrate Anomali more in depth. Can you provide a couple of dates and times this month that would work best for you? We'd also like to see if Commissioner Goulet and Director Plummer might wish to participate.

Again, thanks for your time and look forward to talking again soon.

Thomas P. Oppel

The Mabus Group
1700 K Street, NW
Suite 810 B
Washington, DC 20006
tpoppel@mabusgroup.com
(202) 525-5955 (O)
(603) 304-6767 (C)

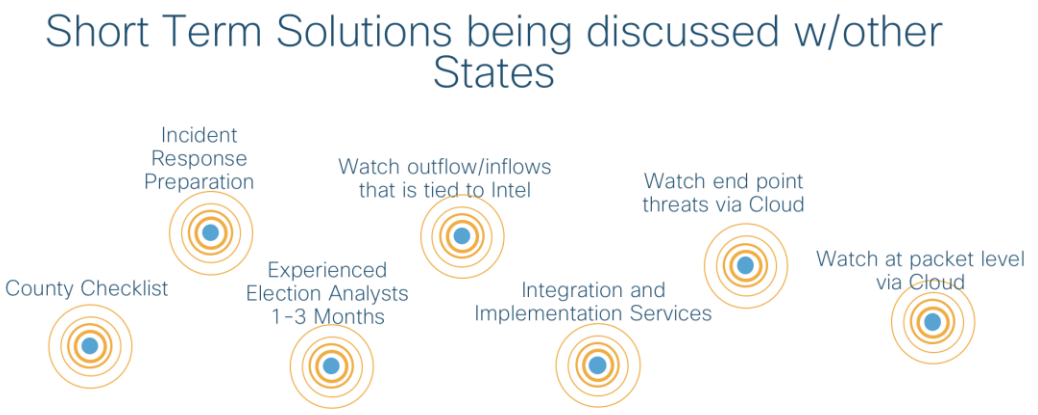
SOS New Hampshire / Cisco Security – 6/25/18

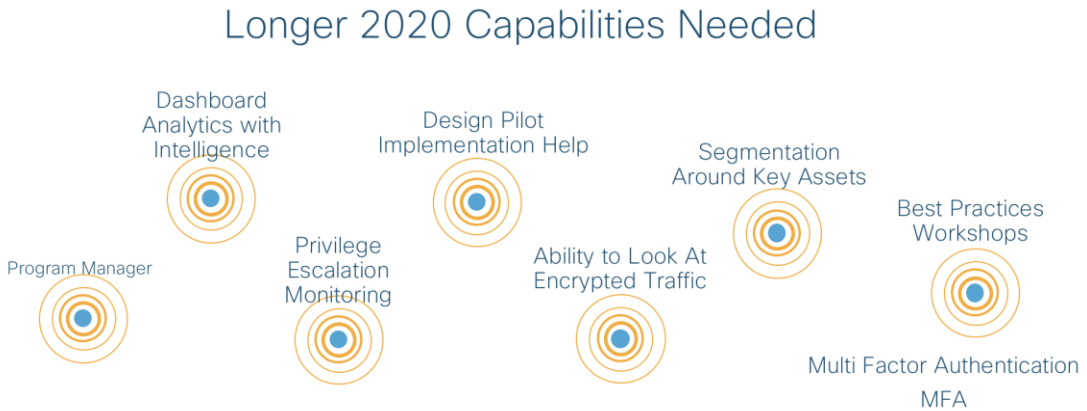
Cisco Attendees:

Jeff Fawcett – Advanced Services Director, Public Sector
James Sarno – State of NH Account Manager
Tanishq Bhalla – Cybersecurity Specialist, New England Public Sector

Agenda:

1) Review of HAVA Grant requirements
2) Open Discussion- Your Status, Concerns…etc.
3) Learnings from other States- Short Term & Longer-term Strategies





Red Team Exercise Description.

The Red Team exercise is a goal-oriented, rather than scope-oriented, security assessment. The scope of the exercise target can be as large as the organization itself, rather than any set of handpicked assets, reflecting real world attacker activities and behavior patterns. The goals and objectives of such an engagement are often defined as compromise of PII, PCI or PI, as defined by industry needs and technical viability. Objectives may include access to a sensitive data source or ongoing access, such as eavesdropping on a channel that may allow for exfiltration of sensitive data. In order to accomplish these objectives, rudimentary online discovery is performed to assess the target attack surface, and open source intelligence gathering is conducted to evaluate personnel and physical site security status. Focusing on the major attack vectors that are included in full Red Team engagements, Attack and Penetration Experts develop a high-level attack plan, including the following vectors:

- External Applications
- Internal Applications
- External Infrastructure
- Internal Infrastructure
- Social Engineering of Personnel and Contractors
- Physical Infiltration of Sites

Scoping for social engineering is approved in advance to ensure selected targets are relevant for this form of testing, and that these targets are unaware of the engagement to confirm true simulation of social engineering attacks.

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Friday, June 29, 2018 12:09 PM
To: Daniel J Cloutier
Cc: Jeff Fawcett (jefawcet); James Sarno (jimsarno); Tanishq Bhalla (tbhalla)
Subject: Thank you & follow up information from meeting with Cisco
Attachments: Red Team Exercise Description.docx

Dear Mr. Cloutier –

Thank you again for meeting with the folks from Cisco (Jeff Fawcett, James Sarno, Tanishq Bhalla) and me on Monday to discuss your goals and initiatives relative to the Secure Election Act. It seems that the State of NH is in good position moving forward. As an FYI, the State of Vermont was interested in what Cisco terms a "Red Team Exercise" in cyber security assessment and asked for a write up that they might use in their response to the federal government. I included a copy of this write up for your information, in case you might find it helpful.

During our conversations, a couple of Cisco capabilities were discussed that seemed to be of interest. Specifically, we discussed the following offerings that could warrant further discussion:

1. DNS security on Roaming devices: https://umbrella.cisco.com/use-cases/off-network-coverage
2. NAC & Network Segmentation: https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html
3. Encrypted Traffic Analytics: https://www.cisco.com/c/en/us/solutions/enterprise-networks/enterprise-network-security/eta.html

The Cisco folks would be happy to come back to present more detailed information on any or all of these issues – in other states they provide an overview and demo of the technology. I have cc'd Jeff, James and Tanishq on this email so you will have direct contact information.

Again, we appreciate your time and look forward to hearing from you!

Have a wonderful weekend.

Jodi

Jodi Grimbilas, President
J Grimbilas Strategic Solutions LLC
(Office) 4 Park Street, Suite 101, Concord
(Mail) PO Box 233, Northwood, NH 03261
(Cell) 603-496-2638
jodi@jgstrategies.com

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Monday, June 25, 2018 2:02 PM
To: Daniel J Cloutier
Subject: RE: Document for Monday meeting with Cisco

HI Mr. Cloutier –

Just checking in. See you at 3pm.

Jodi

From: Jodi Grimbilas
Sent: Saturday, June 23, 2018 4:43 PM
To: 'daniel.cloutier@sos.nh.gov' <daniel.cloutier@sos.nh.gov>
Subject: Document for Monday meeting with Cisco

Hi Mr. Cloutier –

Here is a one-page agenda for the discussion on Monday with Cisco. Again, thank you for making the time.

See you Monday at 3pm.

Jodi

Jodi Grimbilas, President
J Grimbilas Strategic Solutions LLC
(Office) 4 Park Street, Suite 101, Concord
(Mail) PO Box 233, Northwood, NH 03261
(Cell) 603-496-2638
jodi@jgstrategies.com

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Saturday, June 23, 2018 4:43 PM
To: Daniel J Cloutier
Subject: Document for Monday meeting with Cisco
Attachments: NH Election Security.docx

Hi Mr. Cloutier –

Here is a one-page agenda for the discussion on Monday with Cisco. Again, thank you for making the time.

See you Monday at 3pm.

Jodi

Jodi Grimbilas, President
J Grimbilas Strategic Solutions LLC
(Office) 4 Park Street, Suite 101, Concord
(Mail) PO Box 233, Northwood, NH 03261
(Cell) 603-496-2638
jodi@jgstrategies.com

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Friday, June 22, 2018 7:19 AM
To: Jodi Grimbilas
Subject: Accepted: Meeting with Daniel Cloutier & Cisco

Daniel J Cloutier

Subject: Canceled: Meeting with Daniel Cloutier SOS and Cisco
Location: 9 Ratification Way

Start: Tue 6/26/2018 3:00 PM
End: Tue 6/26/2018 3:45 PM
Show Time As: Free

Recurrence: (none)

Organizer: Jodi Grimbilas

Importance: High

Hi Mr. Cloutier –

I will be receiving materials from Cisco, along with names and bios, which I will forward to you ASAP. Thank you for taking the time. I expect there will be three folks from Cisco, plus me.

Have a great day.

Jodi Grimbilas

Daniel J Cloutier

Subject:	Meeting with Daniel Cloutier & Cisco
Location:	9 Ratification Way
Start:	Mon 6/25/2018 3:00 PM
End:	Mon 6/25/2018 3:45 PM
Show Time As:	Tentative
Recurrence:	(none)
Meeting Status:	Not yet responded
Organizer:	Jodi Grimbilas

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Thursday, June 21, 2018 4:13 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

OK – 3pm on Monday in-person works. I should have materials sent to you tomorrow.

I will send out an invite. Thank you for being so patient!

Jodi

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 3:18 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Not usually as there is not as much dialogue in a Webex as you can have in person - although it is up to you. I can do either.

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:47 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

One last question – would a Webex meeting be easier for you instead of in- person?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:45 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Yes

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:33 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

OK – let me check Monday afternoon – would a 3- 3:45 work for you then?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:30 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Monday would be better as I would be able to space my meetings. A half-hour on Tuesday from 2:00PM to 2:30PM is possible which would allow me to work with our Splunk vendor between meetings may work as well.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:12 PM

To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, June 21, 2018 3:18 PM
To: 'Jodi Grimbilas'
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Not usually as there is not as much dialogue in a Webex as you can have in person - although it is up to you. I can do either.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:47 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

One last question – would a Webex meeting be easier for you instead of in- person?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:45 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Yes

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:33 PM

To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

OK – let me check Monday afternoon – would a 3- 3:45 work for you then?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:30 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Monday would be better as I would be able to space my meetings. A half-hour on Tuesday from 2:00PM to 2:30PM is possible which would allow me to work with our Splunk vendor between meetings may work as well.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:12 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Thursday, June 21, 2018 2:47 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

One last question – would a Webex meeting be easier for you instead of in- person?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:45 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Yes

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:33 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

OK – let me check Monday afternoon – would a 3- 3:45 work for you then?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:30 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Monday would be better as I would be able to space my meetings. A half-hour on Tuesday from 2:00PM to 2:30PM is possible which would allow me to work with our Splunk vendor between meetings may work as well.

Thanks,

Dan

Daniel J Cloutier

Assistant Secretary of State

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:12 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, June 21, 2018 2:45 PM
To: 'Jodi Grimbilas'
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Yes

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:33 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

OK – let me check Monday afternoon – would a 3- 3:45 work for you then?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:30 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Monday would be better as I would be able to space my meetings. A half-hour on Tuesday from 2:00PM to 2:30PM is possible which would allow me to work with our Splunk vendor between meetings may work as well.

Thanks,
Dan
Daniel J Cloutier
Assistant Secretary of State

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:12 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Thursday, June 21, 2018 2:33 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

OK – let me check Monday afternoon – would a 3- 3:45 work for you then?

From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:30 PM
To: Jodi Grimbilas <jodi@jgstrategies.com>
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Monday would be better as I would be able to space my meetings. A half-hour on Tuesday from 2:00PM to 2:30PM is possible which would allow me to work with our Splunk vendor between meetings may work as well.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:12 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, June 21, 2018 2:30 PM
To: 'Jodi Grimbilas'
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Monday would be better as I would be able to space my meetings. A half-hour on Tuesday from 2:00PM to 2:30PM is possible which would allow me to work with our Splunk vendor between meetings may work as well.

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State

New Hampshire Department of State
State House, Room 204 - 107 North Main St
Concord, NH 03301-4989
Phone: 603.271.3242 - Fax: 603.271.6316

Information Technology Office
9 Ratification Way, Room 209
Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Jodi Grimbilas [mailto:jodi@jgstrategies.com]
Sent: Thursday, June 21, 2018 2:12 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Thursday, June 21, 2018 2:12 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

I might also be able to coordinate Monday afternoon….(June 25th)

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Jodi Grimbilas <jodi@jgstrategies.com>
Sent: Thursday, June 21, 2018 2:11 PM
To: Daniel J Cloutier
Subject: RE: Meeting with Daniel Cloutier SOS and Cisco

Would 2pm work instead?

Here is my contact info:

Jodi Grimbilas, President
J Grimbilas Strategic Solutions LLC
(Office) 4 Park Street, Suite 101, Concord
(Mail) PO Box 233, Northwood, NH 03261
(Cell) 603-496-2638
jodi@jgstrategies.com

-----Original Appointment-----
From: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco
When: Tuesday, June 26, 2018 3:00 PM-3:45 PM (UTC-05:00) Eastern Time (US & Canada).
Where: 9 Ratification Way

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Thursday, June 21, 2018 2:10 PM
To: Jodi Grimbilas
Subject: Declined: Meeting with Daniel Cloutier SOS and Cisco

Jodi, I attempted to find your number to call. I received our meeting notice for our monthly MS-ISAC call for the same time. I cannot meet at this time.

Daniel J Cloutier

Subject: Meeting with Daniel Cloutier SOS and Cisco
Location: 9 Ratification Way

Start: Tue 6/26/2018 3:00 PM
End: Tue 6/26/2018 3:45 PM
Show Time As: Tentative

Recurrence: (none)

Meeting Status: Not yet responded

Organizer: Jodi Grimbilas

Hi Mr. Cloutier –

I will be receiving materials from Cisco, along with names and bios, which I will forward to you ASAP. Thank you for taking the time. I expect there will be three folks from Cisco, plus me.

Have a great day.

Jodi Grimbilas

CROWDSTRIKE FALCON:
THE NEW STANDARD IN ENDPOINT PROTECTION

ENDPOINT SECURITY BASED ON A SIMPLE, YET POWERFUL APPROACH

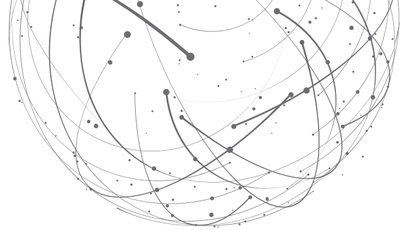
The CrowdStrike Falcon lightweight agent and powerful cloud work seamlessly to deliver real-time protection and visibility — **yes, even when the agent is not connected to the internet.** CrowdStrike Falcon provides robust threat prevention, leveraging artificial intelligence (AI) and machine learning (ML) with advanced detection and response, and integrated threat intelligence — all through a highly intuitive management console.

WHY CROWDSTRIKE FALCON?

COMPLETE PROTECTION
Immediate and effective prevention and detection against all types of attacks — both malware and malware-free — regardless of whether you are online or offline

UNRIVALED VISIBILITY
A "DVR" for your endpoint — nothing is missed. Discover and investigate current and historic endpoint activity in seconds

ULTIMATE EASE OF USE
One cloud-delivered platform that's easy to deploy, configure and maintain — all using a single, lightweight agent



CROWDSTRIKE: TRIED, TESTED, PROVEN

With CrowdStrike, you can be confident that your organization is finally protected from cyberattacks — known or unknown, with or without malware. But don't just take our word for it, see what the experts are saying about **CrowdStrike Falcon:**

"Visionary"

—**GARTNER EPP MAGIC QUADRANT** — JANUARY 2018

"Leader"

—**IDC MARKETSCAPE** — APRIL 2017

"High Score"

—**GARTNER EDR SOLUTIONS** — JUNE 2016

"Strong Performer"

—**FORRESTER WAVE** — OCTOBER, 2016

CROWDSTRIKE CORPORATE HEADQUARTERS

150 MATHILDA PLACE, SUITE 300 SUNNYVALE, CA 94068

info@crowdstrike.com | sales@crowdstrike.com | crowdstrike.com

Experienced a breach? Contact us at (855) 276-9347 or services@crowdstrike.com

CROWDSTRIKE

BUILT TO STOP BREACHES

CLOUD-DELIVERED ENDPOINT PROTECTION

CROWDSTRIKE FALCON:
MAKING THE "IMPOSSIBLE" POSSIBLE

They said it was impossible to provide complete endpoint protection using a single lightweight agent with no impact on user performance. We proved them wrong. With CrowdStrike Falcon's unprecedented real-time visibility, protection and response, **it is now possible to:**

- Prevent both commodity and sophisticated attacks — whether they use malware or not, regardless of whether your endpoints are on or offline.
- Gain real-time endpoint visibility and insight into applications and processes running anywhere in your environment, ensuring that nothing is missed and everything that requires a response, gets one.
- Proactively hunt down advanced threat activity — faster and more effectively than ever before.
- Protect endpoints across all leading platforms, including Windows, macOS and Linux endpoints, data center servers, virtual machines and cloud platforms such as AWS, Azure and Google.
- Retire your legacy antivirus and deploy a next-generation solution that is independently tested and certified as an effective AV replacement.

003377

An Unrivaled Platform

FALCON PREVENT
NEXT-GENERATION ANTIVIRUS (NGAV)

Falcon Prevent™ protects against both malware and malware-free attacks, and is third-party tested and certified, allowing organizations to to confidently replace their legacy AV.

FALCON INSIGHT
ENDPOINT DETECTION AND RESPONSE (EDR)

Falcon Insight™ delivers continuous and comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches can be stopped.

FALCON OVERWATCH
MANAGED THREAT HUNTING

The 24/7 Falcon OverWatch™ team seamlessly augments your in-house security resources to pinpoint malicious activities at the earliest possible stage, stopping adversaries in their tracks.

FALCON DISCOVER
IT HYGIENE

Falcon Discover™ identifies unauthorized systems and applications anywhere in your environment in real time, enabling faster remediation to improve your overall security posture.

FALCON SPOTLIGHT
VULNERABILITY MANAGEMENT

Falcon Spotlight™ offers security teams a continuous and real-time assessment of the vulnerability exposure of their endpoints.

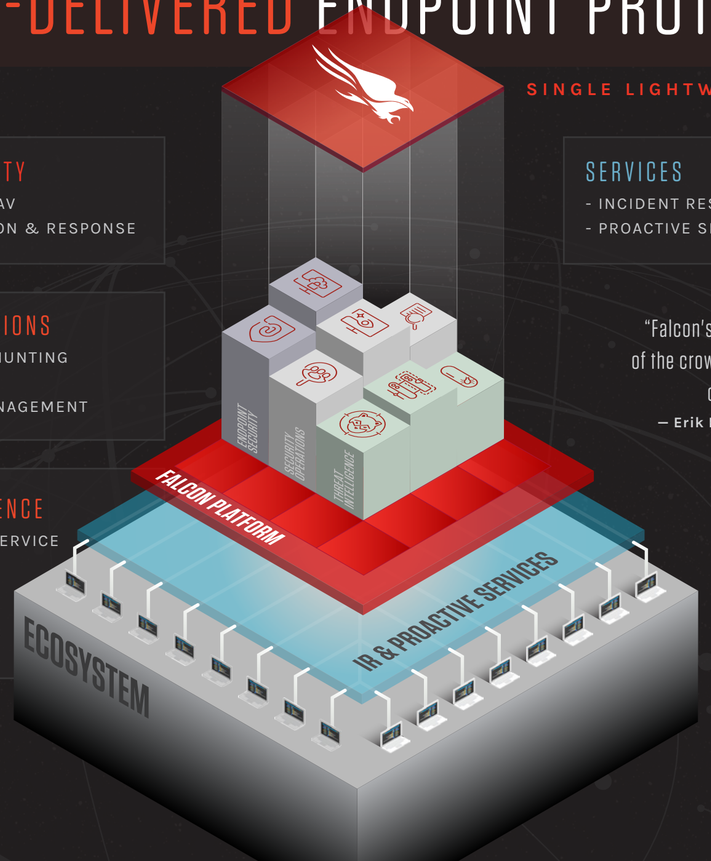
CLOUD-DELIVERED ENDPOINT PROTECTION

SINGLE LIGHTWEIGHT AGENT

ENDPOINT SECURITY
- NEXT GENERATION AV
- ENDPOINT DETECTION & RESPONSE

SECURITY OPERATIONS
- MANAGED THREAT HUNTING
- IT HYGIENE
- VULNERABILITY MANAGEMENT

THREAT INTELLIGENCE
- THREAT ANALYSIS SERVICE
- MALWARE SEARCH
- CYBER THREAT INTELLIGENCE
- MALWARE ANALYSIS



SERVICES
- INCIDENT RESPONSE
- PROACTIVE SERVICES

"Falcon's ability to harness the power of the crowd and of the cloud to protect organizations is tremendous"

— **Erik Hart,** CISO Zebra Technologies

FALCON X
THREAT ANALYSIS SERVICE

Falcon X™ automates threat analysis, enabling security teams to learn from encounters with adversaries and use that knowledge to protect against future attacks.

FALCON INTELLIGENCE
CYBER THREAT INTELLIGENCE

Falcon Intelligence delivers strategic reports and tactical indicators of compromise that provide insight into every aspect of the threat actors that are targeting your organization.

FALCON MALQUERY
MALWARE SEARCH

Falcon MalQuery dramatically increases the speed of malware research while simultaneously enriching the results with threat intelligence, enabling rapid response and protective actions.

FALCON SANDBOX
AUTOMATED MALWARE ANALYSIS

Falcon Sandbox™ provides visibility into malware behavior, automating in-depth file and memory analysis for faster threat protection and response.

IR & PROACTIVE SERVICES

CrowdStrike's pre- and post-incident response (IR) services are available 24/7 to support you before, during or after a breach occurs. These skilled teams deliver the capabilities you need to defend against and respond to security incidents, preventing breaches and optimizing your speed to remediation.

State of New Hampshire
Department of State

Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
Finance@nuharborsecurity.com
1-802-448-4483

P.O. Number: NHSOS-19-SW58

June 12, 2019

Description: SOS Software & Support Renewal	Qty	Price	Total
PP-B-TBEPF-S-A-101 TAP URL Defense & AttDef, TAP Dashboard, Dynamic Reputation, Spam, Virus Protection, Zero-Hour Anti-Virus, Email Firewall, Impostor email, greymail filtering, Smart Search - F-Secure – SaaS, 1-250 12 Months 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	1	19,687.50	$19,687.50
PP-SUP-PS-SME-12 Platinum Level Support -SME 12 Months Support 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	1	0.00	0.00
PP-M-AP-V-B-101 PFPT Threat Response Auto-Pull (AP) Tier 1 – Up to 125 Users	1	4,150.00	4,150.00
PP-PST-PTR-A-101 PFPT Configuration Threat Response	1	0.00	0.00
PP-SUP-PS-S-12 Platinum Level Support – SaaS (Included) – 12 Months Support 125 Users	1	0.00	0.00
Total Systems Quote for this PO			**$23,837.50**

Bill To: (send 2 copies of the invoice please):

New Hampshire Secretary of State
Attn: Paula Penney
State House,
107 North Main Street
Concord, NH, 03301-4989

Ship To:

New Hampshire Secretary of State
Attn: Daniel.Cloutier@sos.nh.gov
9 Ratification Way
Concord, NH, 03301

Telephone: (603) 271-0001
Order Contact: Daniel Cloutier, eMailDaniel.Cloutier@sos.nh.gov, 1-603-271-0001

Use the name "NH Secretary of State" on all license agreements or other documents as required.

Sincerely,

Paula Penney
Assistant Secretary of State

6/12/19
Date

003379

NuHarbor SECURITY

proofpoint

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE June 12, 2019
QUOTE EXPIRES June 15, 2019

TO: Daniel Cloutier
Assistant Secretary of State, Director of IT & Data Security
State of New Hampshire
71 South Fruit Street
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
finance@nuharborsecurity.com
(802) 448-4483

Software & Support Renewal / Upgrade

Line No.	Part No.	Description	Unit Price	Qty	Amount
1	PP-B-TBEPF-S-A-101	TAP URL Defense & AttDef, TAP Dashboard, Dynamic Reputation, Spam, Virus Protection, Zero-Hour Anti-Virus, Email Firewall, Impostor email, greymail filtering, Smart Search - F-Secure - SaaS 1-250, 12 Months 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	19,687.50	1.00	19,687.50
2	PP-SUP-PS-SME-12	Platinum Level Support - SME - 12 months support 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	0.00	1.00	0.00
3	PP-M-AP-V-B-101	PFPT Threat Response Auto-Pull (AP) Tier 1 - Up to 125 Users	4,150.00	1.00	4,150.00
4	PP-PST-PTR-A-101	PFPT Configuration - Threat Response	-	1.00	-
5	PP-SUP-PS-S-12	Platinum Level Support - SaaS (Included) - 12 months support 125 Users	0.00	1.00	0.00
				TOTAL	$23,837.50

12 Month Term Licensing

NuHarbor Security Terms:
Invoice for this purchase shall occur upon Client receiving deliverable. Invoice payments are due net thirty (30) days from date of invoice. Accounts not paid within these terms are subject to a 1% monthly finance charge.
If applicable, Client is responsible for all state sales tax
The Subscription Start Date shall be the date this Order is fully executed.
Once executed by The Bill to Account, this Order is non-cancellable and amounts paid are non-refundable.
Client agrees to the terms and total set forth herein as indicated by the signatures and date of their respective duly authorized representatives below:

Signature

Print Name

Title

Date

State of New Hampshire
Department of State

Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
Finance@nuharborsecurity.com
1-802-448-4483

P.O. Number: NHSOS-19-SW59

June 12, 2019

Description: SOS	Qty	Price	Total
CS-FCSD-SOLN-T2 **Falcon Complete** Advanced Next-Generation Antivirus (Prevent) + Endpoint Detection & Response (Insight) + IT Hygiene (Discover)*Falcon Complete Subscription Included* **List Price 275.75 (per endpoint) Discounted Price 118.65(per endpoint)**	370	118.65	$43,900.50
CS-OW-SVC-T3 **Falcon Overwatch Service** 24x7x365 Managed Hunting Team Included in Falcon Complete	370	0.00	0.00
CS-PE-07 **Threat Graph Standard** Standard Retention (7 Day) Included in Falcon Complete	370	0.00	0.00
CS-Device-SOLN-T3 **Falcon Device Control** Removeable Media Control List Price 9.96 Discounted Price 1.54	370	1.54	569.80
Total Systems Quote for this PO			**$44,470.30**

Bill To: (send 2 copies of the invoice please):

New Hampshire Secretary of State
Attn: Paula Penney
State House,
107 North Main Street
Concord, NH, 03301-4989

Ship To:

New Hampshire Secretary of State
Attn: Daniel.Cloutier@sos.nh.gov
9 Ratification Way
Concord, NH, 03301

Telephone: (603) 271-0001
Order Contact: Daniel Cloutier, eMailDaniel.Cloutier@sos.nh.gov, 1-603-271-0001

Use the name "NH Secretary of State" on all license agreements or other documents as required.

Sincerely,

Paula Penney
Assistant Secretary of State

6/12/19
Date

NuHarbor SECURITY

CROWDSTRIKE

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE June 12, 2019
QUOTE EXPIRES July 12, 2019

TO: Daniel Cloutier
Assistant Secretary of State, Director of IT & Data Security
State of New Hampshire
9 Ratification Way
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
finance@nuharborsecurity.com
(802) 448-4483

Software & Services Renewal

Line No.	Part No.	Description	List Price (per endpoint)	Discounted Price (per endpoint)	Qty	Amount
1	CS-FCSD-SOLN-T2	**Falcon Complete** Advanced Next-Generation Antivirus (Prevent) + Endpoint Detection & Response (Insight) + IT Hygiene (Discover) *Falcon Complete Subscription Included*	275.75	118.65	370.00	43,900.50
2	CS-OW-SVC-T3	**Falcon Overwatch Service** 24x7x365 Managed Hunting Team *Included in Falcon Complete*	-	-	370.00	-
3	CS-PE-07	**Threat Graph Standard** Standard Retention (7 Day) *Included in Falcon Complete*	-	-	370.00	-
4	CS-DEVICE-SOLN-T3	**Falcon Device Control** Removeable Media Control	9.96	1.54	370.00	569.80
		LIST TOTAL	**$ 102,407.46**		**TOTAL**	**$ 44,470.30**

12 Month Term Licensing

NuHarbor Security Terms:
Invoice for this purchase shall occur upon Client receiving deliverable. Invoice payments are due net thirty (30) days from date of invoice. Accounts not paid within these terms are subject to a 1% monthly finance charge.
If applicable, Client is responsible for all state sales tax
The Subscription Start Date shall be the date this Order is fully executed.
Once executed by The Bill to Account, this Order is non-cancellable and amounts paid are non-refundable.
Client agrees to the terms and total set forth herein as indicated by the signatures and date of their respective duly authorized representatives below:

Signature

Print Name

Title

Date

NuHarbor Security
39 River Road, Suite 4
Essex Junction,, VT 05452 US
(800) 917-5719
finance@nuharborsecurity.com
www.nuharborsecurity.com

NuHarbor
SECURITY

INVOICE

BILL TO

New Hampshire Sectretary of State
Attn: Paula Penney
State House, Room 204
107 Main Street
Concord, NH 03301-4989

INVOICE # NHSOS0718-03
DATE 07/24/2018
DUE DATE 08/23/2018
TERMS Net 30

PO
NHSOS-19-SW04

ITEM	DESCRIPTION	QUANTITY	RATE	AMOUNT
CS.EPPADV.SOLN.T3	EPP Advanced (Prevent + Insight + Discover) - Band 3	370	23.23	8,595.10
CS.OW.SVC.T3	Falcon Overwatch Service- Band 3	370	6.35	2,349.50
CS.PE.07	Falcon Platform - Standard Retention (7 Day)	370	6.72	2,486.40
CS.EPPCOMP.SOLN	EPP Complete	370	78.43	29,019.10
CS.DEVICE.SOLN	Falcon Device Control	370	2.12	784.40

REMIT CHECKS TO:
NuHarbor Security Inc.
39 River Road, Suite 4
Essex Junction, VT 05452

BALANCE DUE **$43,234.50**

CROWDSTRIKE

032-NES-3991216-

003383

State of New Hampshire
Department of State

Chief Financial Officer
NuHarbor Security
PO Box 51958
Boston, MA 02205
1-802-448-4483

July 24, 2018

Description: PO # NHSOS-19-SW04	Qty	Price	Total
CS-EPPADV-SOLN-T3 | EPP Advanced (Prevent + Insight + Discover) – Band 3	370	23.23	$ 8,595.10
CS-OW-SVC-T3 | Falcon Overwatch Service – Band 3	370	6.35	2,349.50
CS-PE-07 | Falcon Platform – Standard Retention (7 Day)	370	6.72	2.486.40
CS-EPPCOMP-SOLN | EPP Complete	370	78.43	29,019.10
CS-DEVICE-SOLN | Falcon Device Control	370	2.12	784.40
Total Quote for this PO (See Attached Quote and Document References)			**$43,234.50**

Bill To: (send 2 copies of the invoice please):

New Hampshire Secretary of State
Attn: Paula Penney
State House, Room 204
107 North Main Street
Concord, NH, 03301-4989
Telephone: (603) 271-3242

Ship To:

New Hampshire Secretary of State
Attn: Daniel J. Cloutier
9 Ratification Way
(formerly 71 S Fruit St)
Concord, NH, 03301

Order Contact: Daniel J. Cloutier, Assistant Secretary of State, eMail: Daniel.Cloutier@sos.nh.gov, 1-603-271-0001

Use the name "NH Secretary of State" on all license agreements or other documents as required.

Sincerely,

David M. Scanlan
Deputy Secretary of State

Date 7/24/2018

CROWDSTRIKE

CROWDSTRIKE OVERVIEW

CROWDSTRIKE

„ CROWDSTRIKE GIVES US PROTECTION AND VISIBILITY INTO THREATS THAT WE HAD NO IDEA WERE THERE. THE SIMPLE FACT IS, CROWDSTRIKE IS TECHNICALLY STRONG, THEY DO WHAT THEY SAY THEY'RE GOING TO DO, AND THEY STAND BEHIND THEIR PRODUCT."

- CROWDSTRIKE CUSTOMER SINCE 2015

25K

BREACHES STOPPED
IN 2017

20X

REDUCTION IN
RESOURCE UTILIZATION

75%

INCREASE IN SECURITY
TEAM PRODUCTIVITY

003386

CROWDSTRIKE

BREACH PROLIFERATION

ATTACK SOPHISTICATION

OUTMODED DEFENSES

SOLUTION COMPLEXITY

CROWDSTRIKE

THE KEY TO STOPPING BREACHES

ENDPOINT PROTECTION

MANAGED HUNTING

IR & PROACTIVE SERVICES

THREAT INTELLIGENCE

003388

CROWDSTRIKE

THE KEY TO STOPPING BREACHES

RECOGNITION

Gartner

FORRESTER®

Deloitte.

Forbes

CNBC DISRUPTOR 50

Inc. 500

WORLD ECONOMIC FORUM

AV comparatives

SE Labs

MITRE

CLOUD DELIVERED
ENDPOINT PROTECTION

BENEFITS

01
BETTER
PROTECTION

02
BETTER
PERFORMANCE

03
BETTER
VALUE

003389

THE POWER OF ONE

LIGHTWEIGHT AGENT

003390

CROWDSTRIKE

WHY CROWDSTRIKE

PREVENT ALL ATTACK TYPES

Malware and malware-free
AI and Machine Learning
Behavioral analytics

IMMEDIATE VALUE

A true turnkey solution
Deploy in one day
No consulting services required

CLOUD-DELIVERED
ENDPOINT PROTECTION

REDUCE COST

Consolidate agents
Simplify your architecture
Streamline operations

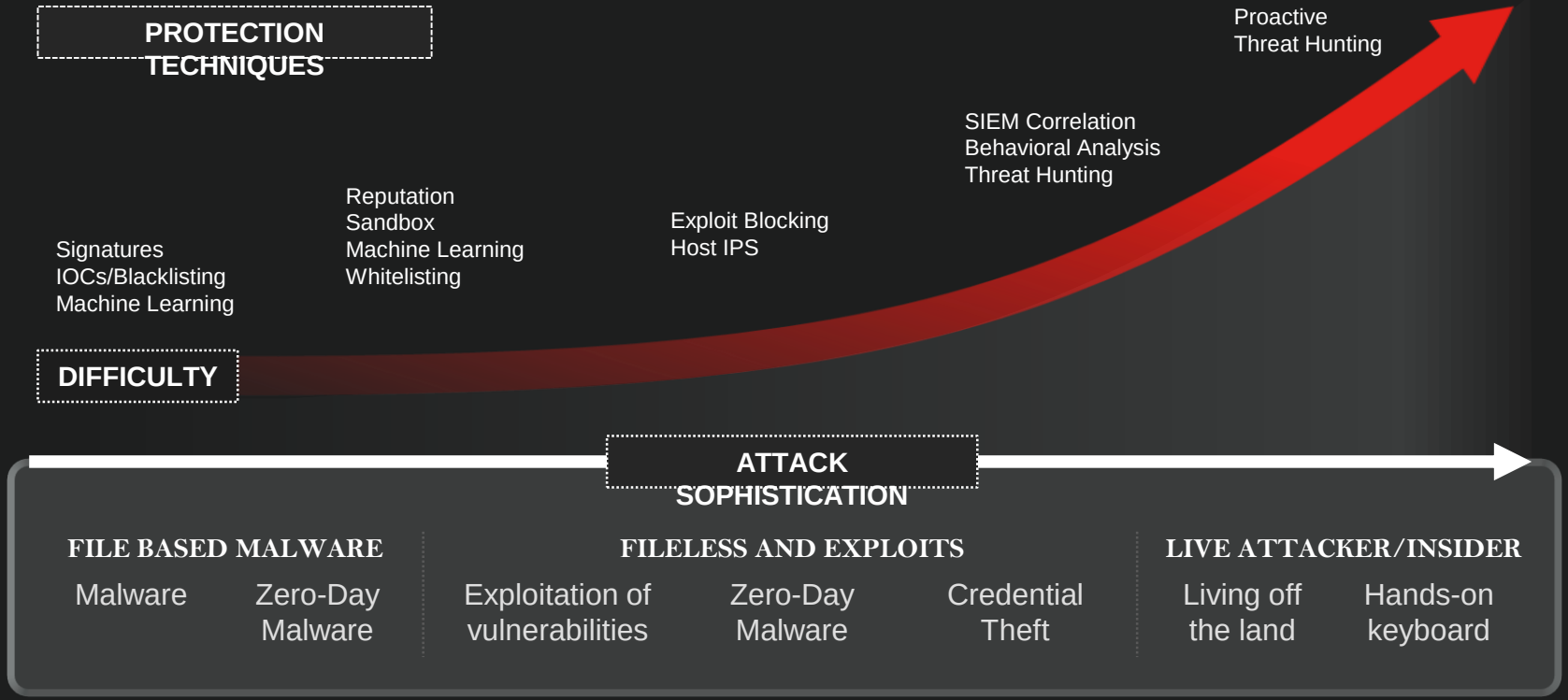
PREVENT THE MEGA BREACH

Don’t let an incident become a breach

003391

CROWDSTRIKE

THE ENDPOINT PROTECTION CHALLENGE



003392

CROWDSTRIKE

THE CROWDSTRIKE SOLUTION

FALCON ENDPOINT PROTECTION

Machine Learning | Exploit Blocking | Behavioral Blocking - Indicators of Attack | EDR | Proactive Threat Hunting | Cyber Threat Intelligence

DIFFICULTY

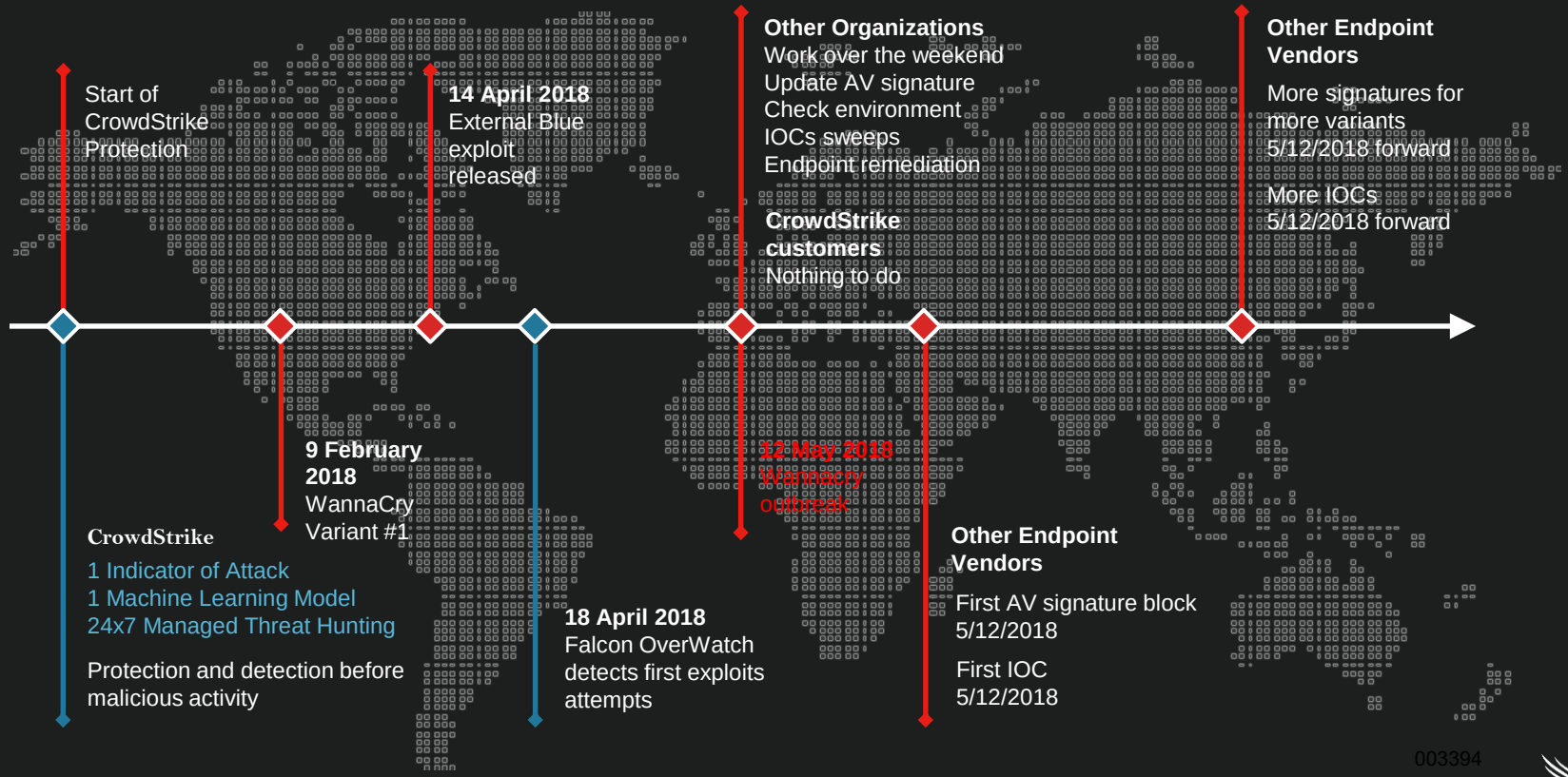
ATTACK SOPHISTICATION

FILE BASED MALWARE		FILELESS AND EXPLOITS			LIVE ATTACKER/INSIDER	
Malware	Zero-Day Malware	Exploitation of vulnerabilities	Zero-Day Malware	Credential Theft	Living off the land	Hands-on keyboard

003393

CROWDSTRIKE

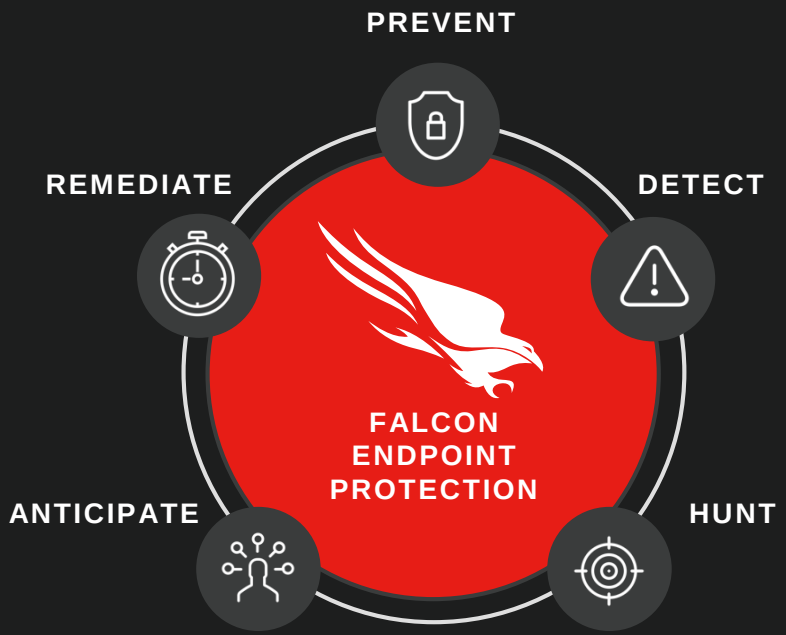
EXAMPLE: WANNACRY



003394

CROWDSTRIKE

A SINGLE AGENT FOR INSTANT SECURITY MATURITY



- 25MB Lightweight agent
- **More than AV replacement:** provides highest level of endpoint protection
- Cloud-based architecture for speed and instant operationalization
- Integrated Threat Intelligence to Outsmart Attackers
- Protection against all type of threats
- Force Multiplier
- Prevent Incidents from Becoming Breaches

003395

CROWDSTRIKE

NEXT-GEN AV – FALCON PREVENT

BENEFITS

AV comparatives APPROVED Business Product 2018

CROWDSTRIKE FALCON CERTIFIED AS LEGACY AV REPLACEMENT

BUSINESS VALUE

Prevents All Types Of Attacks

Protect Against Known/ Unknown Malware

Protect Against Zero-Day Attacks

Eliminate Ransomware

No Signature Updates

No User Impact—Less than 1% CPU overhead

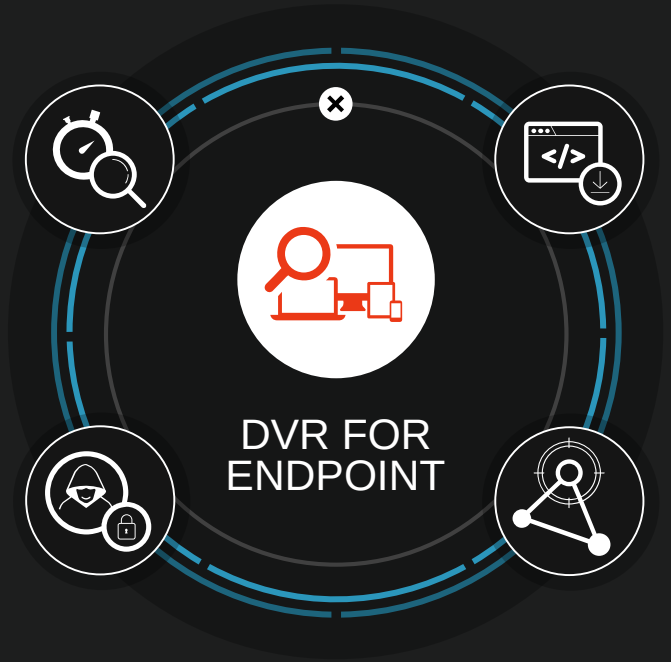
Full Protection Even When Offline

003396

CROWDSTRIKE

ENDPOINT DETECTION AND RESPONSE – FALCON INSIGHT

BENEFITS



BUSINESS VALUE

5 Second Enterprise Search

Protect Against Silent Failure

Reduced Time to Remediation

No Hardware or Storage Costs

CROWDSTRIKE

MANAGED HUNTING – FALCON OVERWATCH

BENEFITS

FINDING THE ADVERSARY
So You Don't Have To

BUSINESS VALUE

Stop the "Mega" Breach

Force Multiplier

Community Immunity

Reduce Alert Fatigue: Focus on What Matters

003398

CROWDSTRIKE

AV comparatives Approved Business Product 2016	Gartner	virustotal	MITRE
99.5% Malware Block Rate	Visionary Quadrant	First Pure ML Engine	ATT&CK Framework
100% Exploit Detection	Highest in Execution	Open to Public Scrutiny	Adversary Emulation
0 False Positives	Highest in Vision	Contribute to Community	Full Protection

COMPLIANCE

PCI Security Standards Council · HIPAA · FFIEC · Privacy Shield Framework · NIST

003399

KEY GARTNER MQ TAKEAWAYS

- A market of Visionaries lead by CrowdStrike
- Gartner's updated definition for endpoint protection validates CrowdStrike strategy
- Cloud delivery, integrated EDR and managed hunting are the way forward

CROWDSTRIKE

THREE SMALL STEPS TO REPLACE YOUR AV

No infrastructure setup

No fine-tuning, rule writing

Install the Falcon Agent

Verify the installation

No reboot

No signatures updates

No scan

Remove legacy products

Financial Institution

77,000 AGENTS
1 DAY

Hospitality Chain

40,000 AGENT
5 DAYS

Technology Company

55,000 AGENTS
5 DAYS

Financial Institution

300,000 AGENTS
90 DAYS

003401

CROWDSTRIKE

WHY
FALCON ENDPOINT PROTECTION

PREVENT ALL ATTACK TYPES

Protect against all types of attacks, from commodity malware to sophisticated attacks, with one solution.

OBTAIN THE BEST PROTECTION EFFORTLESSLY

Works with what you have and who you have – no need for additional investment in hardware or people

ACHIEVE IMMEDIATE SECURITY MATURITY

Instantly achieve the highest level of endpoint protection and breach prevention

GO BEYOND AV REPLACEMENT

Get complete breach prevention, not just AV replacement

003402

CrowdStrike University – Overview & Course Catalog

Revised July 22, 2018

C R O W D S T R I K E S E R V I C E S , I N C .

H E L P I N G Y O U S T O P B R E A C H E S

CrowdStrike University Overview & Course Catalog

CrowdStrike offers professional training and education subscriptions for students from introductory to advanced capabilities. Our education brings out the best in your people, from 24x7 security operations engineers to senior business executives, even those with non-technical responsibilities.

CrowdStrike University Learning Management System (LMS)

CrowdStrike University Learning Management System (LMS) subscription provides students access to:

- **Self-Paced Courses:** Our self-paced courses have been designed to address the fundamentals of a specific topic. Many of these courses are broken up into "digestible" modules – each being 10-15 minutes in length. The modular nature of these courses allows you to stop and start a course as needed or even jump to a specific module topic.

- **Instructor-Led Courses:** Our instructor-led courses cover a variety of intermediate and advanced topics. These courses are delivered via remote meeting technology providing both lecture and hands-on labs. Some courses are available for on-site training sessions. Each instructor-led course has a pre-fixed training credit cost and students must have access to the CrowdStrike University in order to register to any Instructor-led course.

- **How-To Videos/Product Update Video:** In order to give you the latest update to our products, our Product Update Videos are short/informal training videos that address new features, feature changes and other timely topics. Additionally, our How-To Videos series provides access to quick technical tips for the most common problems that you may face.

CrowdStrike University Subscriptions are sold and assigned on person-by-person named basis. Subscriptions are only transferrable with documented change of staff (limited to 10% of number of licenses purchased per year).

Course Delivery

CrowdStrike's experience defending the most important organizations, information and networks powers these education offerings. Experienced instructors and responders teach these courses, drawing on the real-world lessons from these incidents.

Some courses are delivered in a self-paced on-line format, which students can consume at a pace and time that is appropriate for their needs. Others are offered with interactive instruction: some of these instructor-led courses can be delivered via remote meeting technology, and some can be delivered at the client's site.

Courses vary from about 30 minutes for simple how-to topics up to 24 hours for more advanced skills development. Many courses have lab exercises so students can demonstrate their learning; some of those are derived from real incidents.

Courses of up to 16 hours can be offered remotely or on site. On-site courses are conducted eight hours at a time to maximize students' productivity and interaction with the instructors.

Courses that are delivered onsite will include a 4 Training Credit Surcharge for Domestic Travel and 6 Training Credit Surcharge for International Travel.

Both remote and on-site courses have a 6-student minimum and a 15-student maximum.

CrowdStrike University Courses

The following self-paced and instructor-led courses are available in CrowdStrike University. Because of the dynamic nature of the product, courses can be added and removed from the catalog as we adapt the courses to address the latest product feature offerings. For the latest course list, please log into CrowdStrike University and go to the online Course Catalog.

FHT 100 – Falcon Platform Architecture Overview

Course Number:	FHT 100
Course Length:	30 Minutes
Course Cost:	Included with CrowdStrike University subscription
Course Delivery:	Self-paced online
Course Description:	This course describes the various components of the Falcon Platform and how they defend against a typical attack scenario. The course also provides additional details about Falcon Prevent, Falcon Insight, Falcon Intelligence and Falcon Overwatch.

FHT 101 – Falcon Platform Architecture Overview

Course Number: FHT 101

Course Length: 4 Hours

Course Cost: Included with CrowdStrike University subscription

Course Delivery: Self-paced online

Course Description: This course lays the technical foundation to understand installation, configuration and management of the Falcon Platform. This includes a complete GUI-interface walkthrough.

FHT 105 – Sensor Installation, Configuration and Troubleshooting

Course Number: FHT 105

Course Length: 45 Minutes

Course Cost: Included with CrowdStrike University subscription

Course Delivery: Self-paced online

Course Description: This course provides sensor pre-installation considerations, installation examples and options, installation instructions and troubleshooting tips for common installation issues.

FHT 120 – Investigation Fundamentals

Course Number: FHT 120

Course Length: 15 Minutes

Course Cost: Included with CrowdStrike University subscription

Course Delivery: Self-paced online

Course Description: The Investigation Fundamentals course explains what kind of data the Falcon Platform captures, how to access this data through the Falcon Platform interface, and which Falcon Platform apps should be used for different investigation types.

FHT 130 – Falcon Intelligence Fundamentals

Course Number: FHT 130

Course Length: 30 Minutes

Course Cost: Included with CrowdStrike University subscription

Course Delivery: Self-paced online

Course Description: This self-paced course provides students with the fundamentals necessary to make use of the Falcon Intelligence application. It provides an overview of the subscription, with modules about intelligence, reports, threat actors, tailored intelligence, the API and integration points, submitting RFIs and malware for analysis, and summary recommendations.

FHT 201 – Intermediate Falcon Platform for Responders

Course Number: FHT 201

Course Length: 1 Day

Course Cost: 2 training credits

Course Delivery: Virtual instructor Led / On-site instructor Led

Course Description: This course instructs intermediate responders in the best use of the Falcon Platform for incident triage. The course is appropriate for those who use the Falcon Platform on a day to day basis, focused on triaging and responding to alerts. It includes practical labs for students to develop hands-on skills.

FHT 202 – Intermediate Falcon Platform for Hunters

Course Number:	FHT 202
Course Length:	1 Day
Course Cost:	2 training credits
Course Delivery:	Virtual instructor Led / On-site instructor Led
Course Description:	This course instructs intermediate responders in the best use of the Falcon Platform for incident detection using proactive “hunting” investigation. The course is appropriate for those who use the Falcon Platform to find evidence of incidents that did not raise alerts by other means. It includes practical labs for students to develop hands-on skills.

CST 330 – Creating Intelligence with Falcon

Course Number: CST 330

Course Length: 2 Days

Course Cost: 4 training credits

Course Delivery: Virtual instructor Led / On-site instructor Led

Course Description: This two-day instructor-led course introduces the doctrinal concepts of gathering and analyzing information to create intelligence products – it includes Cyber Threat Intelligence methodologies but is more broadly focused on general intelligence doctrine. This is an introductory-level intelligence course and is appropriate for techies and non-techies alike who have little or no experience in intelligence functions and production.

It includes practical labs for students to develop hands-on skills.

This hands-on course is intended for managers, report writers, intelligence consumers, and analysts of all types – there are no prerequisites.

CrowdStrike University Falcon On-boarding Training Kit
A no-charge major initiative

Revised December 19, 2017

CROWDSTRIKE SERVICES, INC.

HELPING YOU STOP BREACHES

Contents

Falcon On-boarding Training Kit

The Falcon On-boarding Training Kit presents course material sufficient to make initial use of the Falcon Platform. This material is appropriate for all who use the Falcon Platform: most of the lessons are aimed at the technical contributor. The material is focused on helping the student efficiently deploy and gain initial value from the features and functionality available to him or her as a user of the technology platform.

All material in the Falcon On-boarding Training Kit is delivered as self-paced online training, allowing students to complete the material at the time and speed convenient for them. It can also be used as post-training reference, for the student retains access to the training platform for the duration of the training subscription. These courses do not include lab exercises; students are expected to cement their knowledge using their organization's access to the Falcon Platform.

Learning Objectives

Once a student has completed all the courses in the curriculum, he or she will be able to:

- Describe the fundamental architecture of the Falcon Platform
- Navigate through the Falcon UI
- Accomplish key functions within the Falcon Platform applications
- Describe the types of data offered in the Executive Summary dashboard
- Describe the user management and Support interface features

This curriculum is not and will not be associated with any certifications.

FHT 090 – Falcon Platform Essentials

Business Value

Achieve basic fluency with the Falcon Platform.

Audience

All customers who will be installing, configuring and managing the Falcon Platform

Security Analyst, SOC Analyst, Security Engineer
IT Security Operations Manager
Security Administrator
Endpoint Security Administrator

Delivery

Self-paced online

Course Length

About 4 hours

Prerequisites

None

Learning Objectives

Students who complete this course should be able to:

- Describe the fundamental architecture of the Falcon Platform
- Describe the Falcon Prevent, Falcon Insight, Falcon Intelligence and Falcon Overwatch applications
- Navigate the Falcon Platform UI
- Accomplish several key functions within the Falcon Platform applications
- Perform basic management of User and Support tasks

Cost per student

Included in Basic training offering

Narrative Description

The Falcon Platform Overview course provides a description of the various components that make up the CrowdStrike Falcon Platform. This includes the Falcon Sensor, CrowdStrike Cloud, Falcon Prevent features, Falcon Insight EDR features, Overwatch, and CrowdStrike intelligence. This course is a great place to start if you are new to CrowdStrike and need a basic orientation of who we are and what we do.

Course Outline

The course follows this agenda:

Falcon Platform product overview
Falcon Sensor / CrowdStrike Cloud
Product installation

Overview of Falcon Insight, Intelligence, Overwatch
Falcon Interface GUI walkthrough
Application walkthroughs
- Activity
- Investigate
- Hosts, Deployment Groups
- Policy management
- Prevention settings
- Dashboards
- Intelligence
- User management
- Support interface

CrowdStrike Falcon Complete Limited Warranty Agreement

This CrowdStrike Limited Warranty Agreement ("Warranty Agreement") is entered into by CrowdStrike, Inc. ("CrowdStrike") and the Customer named below ("Customer") as of the date of the last signature below ("Warranty Effective Date"). This Warranty Agreement is not valid unless signed by both CrowdStrike and Customer. For good and valuable consideration, the sufficiency of which is hereby acknowledged, CrowdStrike and Customer agree as follows:

1. Warranty

1.1. Scope. If Customer experiences a Security Incident in its Protected Environment during a Warranty Period, Customer's sole and exclusive remedy will be under this limited warranty, subject to the terms herein, for the reimbursement of Covered Expenses that directly result from such Security Incident ("Payments") up to a maximum amount not to exceed the applicable Cap set forth in Table 1:

Table 1

The amount paid by Customer for its Falcon Complete subscription that corresponds to the Warranty Period (USD)[Notes 1 and 2]	**"Cap" for the Warranty Period (USD)[Note 3]**
Up to $100,000	$100,000
$100,001 - $250,000	$500,000
$250,001 and above	$1,000,000

Note 1: If Customer's Falcon Complete subscription is not co-terminous with the Warranty Period, for purposes of determining the Cap, the amount Customer paid for the Falcon Complete Subscription(s) shall be prorated to determine the amount paid for the period of time corresponding to the Warranty Period.

Note 2: If Customer purchases its Falcon Complete subscription from a reseller, no later than five (5) days after the start of each Warranty Period, Customer must submit proof of the fee for its Falcon Complete subscription (e.g. reseller's invoice) to CrowdStrike.

Note 3: Aggregate Cyber Extortion Payments during a single Warranty Period shall not exceed $100,000 USD and shall be part of, not in addition to, the applicable Cap.

Aggregate Payments for multiple Security Incidents that have Discovery Dates in a single Warranty Period shall not exceed the Cap for such Warranty Period. This limited warranty extends only to Customer and its Covered Expenses, and unless explicitly agreed by CrowdStrike in writing, does not extend to Customer's affiliates or any of their losses or damages, nor does it extend to any additional third parties (including, but not limited to, suppliers, service providers, end-clients, employees or agents of Customer) or any of their losses or damages.

1.2. Pre-existing and Related Security Incidents. This limited warranty does not extend to Pre-existing Incidents or Related Security Incidents that include a Pre-existing Incident. Except as set forth in this Section 1.2, all Covered Expenses resulting from a Related Security Incident shall be subject to the terms, conditions, exclusions and Cap of the Warranty Period in effect on the Discovery Date of the first discovered Security Incident that forms part of the Related Security Incident.

1.3. Disclaimer. Except for the limited warranty provided in Section 1.1 of this Warranty Agreement and any warranties provided in the Customer Agreement, Falcon Complete (including without limitation the Falcon Platform and Falcon Sensor), is provided AS IS. CROWDSTRIKE AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CROWDSTRIKE AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGMENT WITH RESPECT TO FALCON COMPLETE. THERE IS NO WARRANTY THAT FALCON COMPLETE WILL BE ERROR FREE, OR THAT IT WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS. FALCON COMPLETE IS NOT FOR USE ON ENDPOINTS USED IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, EMERGENCY COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. Customer agrees that it is Customer's responsibility to ensure safe use of Falcon Complete on Endpoints interfacing with such applications and systems.

2. **Reimbursement Qualification**. To be eligible for Payments:
   2.1. During the entirety of each Warranty Period: Customer must have a valid Falcon Complete subscription, Customer's Covered Endpoints must be in the Measured Security Posture (or higher), and Customer's access to the Falcon Platform must be limited to read-only access;
   2.2. At the time the Security Incident first occurs, Customer must be using the most-recent version of the Falcon Sensor on the Endpoint(s) that experienced such Security Incident;
   2.3. The Event Date and Discovery Date of the Security Incident must occur during a Warranty Period;
   2.4. Customer must notify CrowdStrike in accordance with Section 3 below;
   2.5. Customer must be in compliance with its Customer Agreement, including without limitation any payment obligations; and
   2.6. During the entirety of each Warranty Period, Customer must reasonably cooperate with CrowdStrike, including without limitation by implementing all reasonable remediation steps provided by CrowdStrike and providing all reasonably requested information and complying with the reimbursement process set forth in Section 4.

3. **Notification.** If CrowdStrike discovers a Security Incident during a Warranty Period, CrowdStrike shall notify Customer of such Security Incident in accordance with the Falcon Complete Operating Model guide. If Customer discovers a Security Incident during a Warranty Period, Customer shall notify CrowdStrike of such Security Incident by sending an email to warrantyclaim@crowdstrike.com no later than three (3) days after the Discovery Date of such Security Incident. Customer shall have fifteen (15) days from (a) the date CrowdStrike provides notice of a Security Incident to Customer, or (b) Customer provides notice of a Security Incident to CrowdStrike, to notify CrowdStrike of Customer's intent to request Payments by sending an email to warrantyclaim@crowdstrike.com ("Reimbursement Request").

4. **Reimbursement Request Process**.
   4.1. Reimbursement Request Requirements. A separate Reimbursement Request must be submitted to CrowdStrike for each Security Incident. Such Reimbursement Request shall include all information available to Customer regarding the Security Incident.
   4.2. Submission of Reimbursement Request. CrowdStrike shall review the Reimbursement Request and Customer shall provide any additional information reasonably requested by CrowdStrike at any time. By submitting the Reimbursement Request to CrowdStrike, Customer authorizes CrowdStrike to share any information that is reasonably necessary to assess the validity of the Reimbursement Request with Carrier, provided Carrier is under an obligation to keep such information confidential. Reimbursement Requests made under this limited warranty are subject to Carrier's standards of review. If Carrier denies coverage to CrowdStrike for any Reimbursement Request, notwithstanding anything to the contrary in this Warranty Agreement, CrowdStrike shall have no obligation to make any Payments for such Reimbursement Request to Customer.
   4.3. Payments. CrowdStrike shall have no obligation to make Payments that are prohibited by law. Customer shall submit proof of Covered Expenses in accordance with CrowdStrike's instructions. During the term of the Warranty Agreement and for a period of three (3) years thereafter, CrowdStrike shall have the right at its own expense to inspect, and Customer shall maintain and provide, Customer's records related to such Covered Expenses upon reasonable written request during regular business hours.

5. **Choice of Law; Arbitration**. Notwithstanding any dispute resolution or venue provisions in the Customer Agreement: (1): any dispute, claim, or controversy arising out of or relating to this Warranty Agreement or the existence, breach, termination, enforcement, interpretation, or validity of this Warranty Agreement, including the determination of the scope or applicability of this arbitration clause, (each, a "Dispute") shall be referred to and finally resolved by arbitration under the rules of the American Arbitration Association in force on the date when the notice of arbitration is submitted in accordance with such rules (which rules are deemed to be incorporated by reference into this clause) on the basis that the governing law is the law of the State of California, USA; and (2) any Customer claims under the Customer Agreement that are in any way related to a Dispute or Falcon Complete shall also be subject to this arbitration provision. The seat, or legal place, of arbitration shall be Santa Clara, California, USA. The arbitral panel shall consist of three (3) arbitrators, selected as follows: each party shall appoint one (1) arbitrator; and those two (2)

arbitrators shall discuss and select the third arbitrator. If the two party-appointed arbitrators are unable to agree on a third arbitrator, the third arbitrator shall be selected in accordance with the applicable rules of the arbitration body. Each arbitrator shall be independent of all parties to the arbitration and shall have suitable experience and knowledge in the subject matter of the Dispute. Judgment upon the award so rendered may be entered in a court having jurisdiction or application may be made to such court for judicial acceptance of any award and an order of enforcement, as the case may be. The language to be used in the arbitral proceedings shall be English.

6. **Insurance**. CrowdStrike has obtained one or more insurance policies to cover its obligations under this Warranty Agreement. Customer is not an insured under such insurance policies. Where approved by CrowdStrike, Customer agrees to communicate directly with Carrier regarding Reimbursement Requests (including without limitation obtaining prior written approvals) and to provide the same information and cooperation required under this Warranty Agreement to any Carrier issuing such an insurance policy.

7. **General**

7.1. Entire Agreement. This Warranty Agreement constitutes the entire agreement between Customer and CrowdStrike concerning the subject matter of this Warranty Agreement and it supersedes any prior or concurrent proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter. For the avoidance of doubt, this Warranty Agreement is in addition to the Customer Agreement and except as expressly set forth herein, nothing in this Warranty Agreement is intended to supersede, modify or amend the Customer Agreement, including the warranties therein.

7.2. Limitation of Liability. IN NO EVENT WILL CROWDSTRIKE OR ITS SUPPLIERS BE LIABLE (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR ANY LOST PROFITS, LOST BUSINESS OPPORTUNITIES, BUSINESS INTERRUPTION, LOST DATA, DATA RESTORATION, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; AND IN NO EVENT SHALL CROWDSTRIKE'S LIABILITY UNDER OR ARISING FROM THIS WARRANTY AGREEMENT EXCEED CUSTOMER'S CAP AS SET FORTH IN SECTION 1.1 ABOVE FOR THE WARRANTY PERIOD IN EFFECT AT THE TIME OF THE EVENT GIVING RISE TO SUCH LIABILITY. Multiple claims or Security Incidents shall not expand the limitation specified in the foregoing sentence. Any Payments, damages or losses paid under this Warranty Agreement shall accrue towards any liability cap set forth in the Customer Agreement.

7.3. Term; Termination; Assignment. This Warranty Agreement shall commence on the Warranty Effective Date and continue for one year thereafter ("Initial Warranty Period"). Thereafter, unless terminated earlier in accordance with this Section 7.3, this Warranty Agreement shall automatically renew for successive one-year periods provided Customer's Falcon Complete subscription and Customer Agreement have not terminated or expired (each, a "Renewal Warranty Period"). Unless otherwise specified herein, this Warranty Agreement shall remain effective until terminated in accordance with this Section or the Customer Agreement. CrowdStrike can provide written notice of termination of this Warranty Agreement at any time provided such termination shall be effective as of the last day of Customer's then-current Warranty Period. Termination of the Customer Agreement shall terminate this Warranty Agreement. Termination of this Warranty Agreement shall not terminate the Customer Agreement. Customer may not assign this Warranty Agreement without the prior written consent of CrowdStrike, except to an affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets provided Customer provides CrowdStrike with notice of any such assignment no later than thirty (30) days after such assignment or change in control event is public. Any assignment in violation of this Section shall be void and shall void this limited warranty. Subject to the foregoing, all rights and obligations of the parties under this Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

7.4. Except to the extent a Reimbursement Request arises out of an event that is later determined (1) not a Security Incident, or (2) to relate to a Pre-Existing Incident, CrowdStrike hereby waives any and all rights it has or may have to reimbursement of Payments from Customer. Customer shall promptly (but in no event later than 30 days after written notice) reimburse CrowdStrike for all Payments related to a Reimbursement Request that arises out of an event that is later determined not be a Security Incident or that relates to a Pre-Existing Incident.

8. **Definitions**.
   8.1. **"Carrier"** means the insurance carrier underwriting this warranty.
   8.2. **"Compliance Action"** means (1) a request for information, civil investigative demand, administrative action or civil proceeding brought by a federal or state government entity or agency against Customer, or (2) an action brought by, or written demand from, a payment card association seeking an assessment, fee, fine or penalty for a violation of the PCI Data Security Standard.
   8.3. **"Covered Expenses**" means solely (and to the exclusion of all other fees, expenses, losses, settlements and damages) the following reasonable and necessary fees and expenses to the extent incurred by Customer as a result of a Security Incident: (1) Forensic Investigation Expenses; (2) Legal Consultation Expenses; (3) Post-Security Incident Expenses; (4) Public Relations Expenses; and (5) Cyber Extortion Payments. The foregoing fees and expenses constitute "Covered Expenses" only if: (1) incurred by Customer after having obtained CrowdStrike's prior written approval to obtain such services or incur such expenditures; (2) invoiced by a third-party provider that has been preapproved in writing by CrowdStrike; (3) incurred by Customer within one (1) year following the Discovery Date of the applicable Security Incident; and (4) payment and/or reimbursement does not violate any applicable domestic or foreign law, statute, regulation or rule as determined by CrowdStrike in its sole discretion.
   8.4. **"Covered Endpoint"** means any Endpoint that has the Falcon Sensor installed on it.
   8.5. **"Customer Agreement**" means the agreement between CrowdStrike and Customer governing Customer's Falcon Complete subscription.
   8.6. **"Cyber Extortion Payment"** means money, cryptocurrencies (including the cost to obtain cryptocurrency) or other consideration that Customer surrenders to a natural person or group believed to be responsible for a Security Incident in order to resolve such Security Incident, and that is preapproved in writing by CrowdStrike.
   8.7. **"Discovery Date"** means the earlier of (1) the date Customer first discovers the Security Incident or (2) the date CrowdStrike first discovers the Security Incident.
   8.8. **"Endpoint"** means any physical or virtual device that is under ownership, operation or control of, or is leased by, Customer.

   8.9. **"Event Date"** means the date the Security Incident or Pre-existing Incident first occurred; provided, however, that each Security Incident that forms part of a Related Security Incident shall be deemed to have the Event Date of the earliest Security Incident or Pre-existing Incident (if applicable) that forms part of the Related Security Incident.
   8.10. **"Falcon Complete"** means: (1) EPP Advanced (Prevent + Insight + Discover); (2) Falcon Platform; (3) OverWatch; and (4) Falcon Complete Team.
   8.11. **"Falcon Platform"** means CrowdStrike's cloud software referred to as the Falcon Platform or Threat Graph.
   8.12. **"Falcon Sensor"** means CrowdStrike's then-current Endpoint application for the Falcon Platform.
   8.13. **"Forensic Investigation Expenses"** means fees and expenses incurred by Customer to conduct an investigation (including a forensic investigation) to determine the cause and extent of a Security Incident.
   8.14. **"Legal Consultation Expenses"** means fees and expenses incurred by Customer to obtain data security-related legal advice after a Security Incident, including, without limitation advice related to notification content and requirements. Legal Consultation Expenses do not include any fees or expenses incurred in connection with the response to or defense of any actual, anticipated or threatened suit, action, proceeding, litigation or Compliance Action against the Customer.
   8.15. **"Measured Security Posture"** means the configurations, settings, actions and remediations described in the then-current Falcon Complete Operating Model guide as "measured".
   8.16. **"Personnel"** means Customer's employees, vendors and contractors.
   8.17. **"Physical Event"** means fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, an act of God, loss or theft of a physical Endpoint, or any other physical event, however caused.
   8.18. **"Post-Security Incident Expenses"** means fees and expenses incurred by Customer for (1) notifying individuals whose personally identifiable information may have been compromised by a Security Incident (including the cost

of printing and mailing) and (2) identity theft call center assistance, identity restoration services, credit file or identity monitoring and/or victim expense reimbursement insurance made available to such notified individuals.

8.19. **"Pre-existing Incident"** means any unauthorized access to the operating system of an Endpoint that occurs either (1) before such Endpoint becomes a Covered Endpoint in the Protected Environment; or (2) before Customer's Initial Warranty Period.

8.20. **"Protected Environment"** means Customer's Covered Endpoints that are in the Measured Security Posture (or higher) and monitored by the CrowdStrike's Falcon Complete Team.

8.21. **"Public Relations Expenses"** means fees and expenses incurred by Customer for a public relations firm to advise the Customer on minimizing the harm to Customer and restoring public confidence in Customer after a Security Incident.

8.22. **"Related Security Incident"** means, collectively, the same, continuous, related or repeated Pre-existing Incidents and/or Security Incidents.

8.23. **"Security Incident"** means unauthorized access by a Third Party to the operating system of a Covered Endpoint in the Protected Environment that results in the malicious exfiltration, destruction and/or irreversible encryption of Customer data that Customer reasonably believes has value in excess of $5,000. Notwithstanding the foregoing, unauthorized access arising out of or resulting directly or indirectly from any of the following events does not constitute a Security Incident: (a) Customer whitelisting a Covered Endpoint or process; (b) Customer altering or instructing CrowdStrike to alter configurations such that a Covered Endpoint falls below the Measured Security Posture; (c) Customer's failure to follow CrowdStrike's prevention or remediation instructions; (d) Customer's modification or alteration of Falcon Complete; (e) any fraudulent, criminal or malicious act of Customer or its Personnel, or any intentional or knowing violation of the law by Customer or its Personnel; (f) any Physical Event and/or (g) any form of Unrest.

8.24. **"Third Party"** means any entity or person except Customer and Personnel.

8.25. **"Unrest"** means strike or similar labor action, war, invasion, military action (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events.

8.26. **"Warranty Period"** means the Initial Warranty Period or a Renewal Warranty Period (both defined in Section 7.3), as applicable.

BY THE SIGNATURES BELOW THIS WARRANTY AGREEMENT IS AGREED TO AS OF THE WARRANTY EFFECTIVE DATE:

CROWDSTRIKE SERVICES, INC.		**CUSTOMER:**	State of New Hampshire (Provide complete legal entity name)
By:	Mike Forman	By:	DocuSigned by: David M Scanlan 633D6FEA1A6C412...
Name:	**Mike Forman**	Name:	David M Scanlan
Title:	**V.P. Corporate Controller**	Title:	Deputy Secretary of State
Date:	12/4/2018	Date:	12/4/2018
Address	150 Mathilda Place, Third Floor Sunnyvale, CA 94086	Address:	107 N Main St Concord, New Hampshire 03301-4951

CrowdStrike Falcon Complete Limited Warranty Agreement

This CrowdStrike Limited Warranty Agreement ("Warranty Agreement") is entered into by CrowdStrike, Inc. ("CrowdStrike") and the Customer named below ("Customer") as of the date of the last signature below ("Warranty Effective Date"). This Warranty Agreement is not valid unless signed by both CrowdStrike and Customer. For good and valuable consideration, the sufficiency of which is hereby acknowledged, CrowdStrike and Customer agree as follows:

1. Warranty

1.1. Scope. If Customer experiences a Security Incident in its Protected Environment during a Warranty Period, Customer's sole and exclusive remedy will be under this limited warranty, subject to the terms herein, for the reimbursement of Covered Expenses that directly result from such Security Incident ("Payments") up to a maximum amount not to exceed the applicable Cap set forth in Table 1:

Table 1

The amount paid by Customer for its Falcon Complete subscription that corresponds to the Warranty Period (USD)[Notes 1 and 2]	**"Cap" for the Warranty Period (USD)[Note 3]**
Up to $100,000	$100,000
$100,001 - $250,000	$500,000
$250,001 and above	$1,000,000

Note 1: If Customer's Falcon Complete subscription is not co-terminous with the Warranty Period, for purposes of determining the Cap, the amount Customer paid for the Falcon Complete Subscription(s) shall be prorated to determine the amount paid for the period of time corresponding to the Warranty Period.

Note 2: If Customer purchases its Falcon Complete subscription from a reseller, no later than five (5) days after the start of each Warranty Period, Customer must submit proof of the fee for its Falcon Complete subscription (e.g. reseller's invoice) to CrowdStrike.

Note 3: Aggregate Cyber Extortion Payments during a single Warranty Period shall not exceed $100,000 USD and shall be part of, not in addition to, the applicable Cap.

Aggregate Payments for multiple Security Incidents that have Discovery Dates in a single Warranty Period shall not exceed the Cap for such Warranty Period. This limited warranty extends only to Customer and its Covered Expenses, and unless explicitly agreed by CrowdStrike in writing, does not extend to Customer's affiliates or any of their losses or damages, nor does it extend to any additional third parties (including, but not limited to, suppliers, service providers, end-clients, employees or agents of Customer) or any of their losses or damages.

1.2. Pre-existing and Related Security Incidents. This limited warranty does not extend to Pre-existing Incidents or Related Security Incidents that include a Pre-existing Incident. Except as set forth in this Section 1.2, all Covered Expenses resulting from a Related Security Incident shall be subject to the terms, conditions, exclusions and Cap of the Warranty Period in effect on the Discovery Date of the first discovered Security Incident that forms part of the Related Security Incident.

1.3. Disclaimer. Except for the limited warranty provided in Section 1.1 of this Warranty Agreement and any warranties provided in the Customer Agreement, Falcon Complete (including without limitation the Falcon Platform and Falcon Sensor), is provided AS IS. CROWDSTRIKE AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CROWDSTRIKE AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGMENT WITH RESPECT TO FALCON COMPLETE. THERE IS NO WARRANTY THAT FALCON COMPLETE WILL BE ERROR FREE, OR THAT IT WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS. FALCON COMPLETE IS NOT FOR USE ON ENDPOINTS USED IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, EMERGENCY COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. Customer agrees that it is Customer's responsibility to ensure safe use of Falcon Complete on Endpoints interfacing with such applications and systems.

2. **Reimbursement Qualification**. To be eligible for Payments:
   2.1. During the entirety of each Warranty Period: Customer must have a valid Falcon Complete subscription, Customer's Covered Endpoints must be in the Measured Security Posture (or higher), and Customer's access to the Falcon Platform must be limited to read-only access;
   2.2. At the time the Security Incident first occurs, Customer must be using the most-recent version of the Falcon Sensor on the Endpoint(s) that experienced such Security Incident;
   2.3. The Event Date and Discovery Date of the Security Incident must occur during a Warranty Period;
   2.4. Customer must notify CrowdStrike in accordance with Section 3 below;
   2.5. Customer must be in compliance with its Customer Agreement, including without limitation any payment obligations; and
   2.6. During the entirety of each Warranty Period, Customer must reasonably cooperate with CrowdStrike, including without limitation by implementing all reasonable remediation steps provided by CrowdStrike and providing all reasonably requested information and complying with the reimbursement process set forth in Section 4.

3. **Notification.** If CrowdStrike discovers a Security Incident during a Warranty Period, CrowdStrike shall notify Customer of such Security Incident in accordance with the Falcon Complete Operating Model guide. If Customer discovers a Security Incident during a Warranty Period, Customer shall notify CrowdStrike of such Security Incident by sending an email to warrantyclaim@crowdstrike.com no later than three (3) days after the Discovery Date of such Security Incident. Customer shall have fifteen (15) days from (a) the date CrowdStrike provides notice of a Security Incident to Customer, or (b) Customer provides notice of a Security Incident to CrowdStrike, to notify CrowdStrike of Customer's intent to request Payments by sending an email to warrantyclaim@crowdstrike.com ("Reimbursement Request").

4. **Reimbursement Request Process**.
   4.1. Reimbursement Request Requirements. A separate Reimbursement Request must be submitted to CrowdStrike for each Security Incident. Such Reimbursement Request shall include all information available to Customer regarding the Security Incident.
   4.2. Submission of Reimbursement Request. CrowdStrike shall review the Reimbursement Request and Customer shall provide any additional information reasonably requested by CrowdStrike at any time. By submitting the Reimbursement Request to CrowdStrike, Customer authorizes CrowdStrike to share any information that is reasonably necessary to assess the validity of the Reimbursement Request with Carrier, provided Carrier is under an obligation to keep such information confidential. Reimbursement Requests made under this limited warranty are subject to Carrier's standards of review. If Carrier denies coverage to CrowdStrike for any Reimbursement Request, notwithstanding anything to the contrary in this Warranty Agreement, CrowdStrike shall have no obligation to make any Payments for such Reimbursement Request to Customer.
   4.3. Payments. CrowdStrike shall have no obligation to make Payments that are prohibited by law. Customer shall submit proof of Covered Expenses in accordance with CrowdStrike's instructions. During the term of the Warranty Agreement and for a period of three (3) years thereafter, CrowdStrike shall have the right at its own expense to inspect, and Customer shall maintain and provide, Customer's records related to such Covered Expenses upon reasonable written request during regular business hours.

5. **Choice of Law; Arbitration**. Notwithstanding any dispute resolution or venue provisions in the Customer Agreement: (1): any dispute, claim, or controversy arising out of or relating to this Warranty Agreement or the existence, breach, termination, enforcement, interpretation, or validity of this Warranty Agreement, including the determination of the scope or applicability of this arbitration clause, (each, a "Dispute") shall be referred to and finally resolved by arbitration under the rules of the American Arbitration Association in force on the date when the notice of arbitration is submitted in accordance with such rules (which rules are deemed to be incorporated by reference into this clause) on the basis that the governing law is the law of the State of California, USA; and (2) any Customer claims under the Customer Agreement that are in any way related to a Dispute or Falcon Complete shall also be subject to this arbitration provision. The seat, or legal place, of arbitration shall be Santa Clara, California, USA. The arbitral panel shall consist of three (3) arbitrators, selected as follows: each party shall appoint one (1) arbitrator; and those two (2)

arbitrators shall discuss and select the third arbitrator. If the two party-appointed arbitrators are unable to agree on a third arbitrator, the third arbitrator shall be selected in accordance with the applicable rules of the arbitration body. Each arbitrator shall be independent of all parties to the arbitration and shall have suitable experience and knowledge in the subject matter of the Dispute. Judgment upon the award so rendered may be entered in a court having jurisdiction or application may be made to such court for judicial acceptance of any award and an order of enforcement, as the case may be. The language to be used in the arbitral proceedings shall be English.

6. **Insurance**. CrowdStrike has obtained one or more insurance policies to cover its obligations under this Warranty Agreement. Customer is not an insured under such insurance policies. Where approved by CrowdStrike, Customer agrees to communicate directly with Carrier regarding Reimbursement Requests (including without limitation obtaining prior written approvals) and to provide the same information and cooperation required under this Warranty Agreement to any Carrier issuing such an insurance policy.

7. **General**

7.1. Entire Agreement. This Warranty Agreement constitutes the entire agreement between Customer and CrowdStrike concerning the subject matter of this Warranty Agreement and it supersedes any prior or concurrent proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter. For the avoidance of doubt, this Warranty Agreement is in addition to the Customer Agreement and except as expressly set forth herein, nothing in this Warranty Agreement is intended to supersede, modify or amend the Customer Agreement, including the warranties therein.

7.2. Limitation of Liability. IN NO EVENT WILL CROWDSTRIKE OR ITS SUPPLIERS BE LIABLE (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR ANY LOST PROFITS, LOST BUSINESS OPPORTUNITIES, BUSINESS INTERRUPTION, LOST DATA, DATA RESTORATION, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; AND IN NO EVENT SHALL CROWDSTRIKE'S LIABILITY UNDER OR ARISING FROM THIS WARRANTY AGREEMENT EXCEED CUSTOMER'S CAP AS SET FORTH IN SECTION 1.1 ABOVE FOR THE WARRANTY PERIOD IN EFFECT AT THE TIME OF THE EVENT GIVING RISE TO SUCH LIABILITY. Multiple claims or Security Incidents shall not expand the limitation specified in the foregoing sentence. Any Payments, damages or losses paid under this Warranty Agreement shall accrue towards any liability cap set forth in the Customer Agreement.

7.3. Term; Termination; Assignment. This Warranty Agreement shall commence on the Warranty Effective Date and continue for one year thereafter ("Initial Warranty Period"). Thereafter, unless terminated earlier in accordance with this Section 7.3, this Warranty Agreement shall automatically renew for successive one-year periods provided Customer's Falcon Complete subscription and Customer Agreement have not terminated or expired (each, a "Renewal Warranty Period"). Unless otherwise specified herein, this Warranty Agreement shall remain effective until terminated in accordance with this Section or the Customer Agreement. CrowdStrike can provide written notice of termination of this Warranty Agreement at any time provided such termination shall be effective as of the last day of Customer's then-current Warranty Period. Termination of the Customer Agreement shall terminate this Warranty Agreement. Termination of this Warranty Agreement shall not terminate the Customer Agreement. Customer may not assign this Warranty Agreement without the prior written consent of CrowdStrike, except to an affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets provided Customer provides CrowdStrike with notice of any such assignment no later than thirty (30) days after such assignment or change in control event is public. Any assignment in violation of this Section shall be void and shall void this limited warranty. Subject to the foregoing, all rights and obligations of the parties under this Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

7.4. Except to the extent a Reimbursement Request arises out of an event that is later determined (1) not a Security Incident, or (2) to relate to a Pre-Existing Incident, CrowdStrike hereby waives any and all rights it has or may have to reimbursement of Payments from Customer. Customer shall promptly (but in no event later than 30 days after written notice) reimburse CrowdStrike for all Payments related to a Reimbursement Request that arises out of an event that is later determined not be a Security Incident or that relates to a Pre-Existing Incident.

8. **Definitions**.
   8.1. **"Carrier"** means the insurance carrier underwriting this warranty.
   8.2. **"Compliance Action"** means (1) a request for information, civil investigative demand, administrative action or civil proceeding brought by a federal or state government entity or agency against Customer, or (2) an action brought by, or written demand from, a payment card association seeking an assessment, fee, fine or penalty for a violation of the PCI Data Security Standard.
   8.3. **"Covered Expenses**" means solely (and to the exclusion of all other fees, expenses, losses, settlements and damages) the following reasonable and necessary fees and expenses to the extent incurred by Customer as a result of a Security Incident: (1) Forensic Investigation Expenses; (2) Legal Consultation Expenses; (3) Post-Security Incident Expenses; (4) Public Relations Expenses; and (5) Cyber Extortion Payments. The foregoing fees and expenses constitute "Covered Expenses" only if: (1) incurred by Customer after having obtained CrowdStrike's prior written approval to obtain such services or incur such expenditures; (2) invoiced by a third-party provider that has been preapproved in writing by CrowdStrike; (3) incurred by Customer within one (1) year following the Discovery Date of the applicable Security Incident; and (4) payment and/or reimbursement does not violate any applicable domestic or foreign law, statute, regulation or rule as determined by CrowdStrike in its sole discretion.
   8.4. **"Covered Endpoint"** means any Endpoint that has the Falcon Sensor installed on it.
   8.5. **"Customer Agreement**" means the agreement between CrowdStrike and Customer governing Customer's Falcon Complete subscription.
   8.6. **"Cyber Extortion Payment"** means money, cryptocurrencies (including the cost to obtain cryptocurrency) or other consideration that Customer surrenders to a natural person or group believed to be responsible for a Security Incident in order to resolve such Security Incident, and that is preapproved in writing by CrowdStrike.
   8.7. **"Discovery Date"** means the earlier of (1) the date Customer first discovers the Security Incident or (2) the date CrowdStrike first discovers the Security Incident.
   8.8. **"Endpoint"** means any physical or virtual device that is under ownership, operation or control of, or is leased by, Customer.

   8.9. **"Event Date"** means the date the Security Incident or Pre-existing Incident first occurred; provided, however, that each Security Incident that forms part of a Related Security Incident shall be deemed to have the Event Date of the earliest Security Incident or Pre-existing Incident (if applicable) that forms part of the Related Security Incident.
   8.10. **"Falcon Complete"** means: (1) EPP Advanced (Prevent + Insight + Discover); (2) Falcon Platform; (3) OverWatch; and (4) Falcon Complete Team.
   8.11. **"Falcon Platform"** means CrowdStrike's cloud software referred to as the Falcon Platform or Threat Graph.
   8.12. **"Falcon Sensor"** means CrowdStrike's then-current Endpoint application for the Falcon Platform.
   8.13. **"Forensic Investigation Expenses"** means fees and expenses incurred by Customer to conduct an investigation (including a forensic investigation) to determine the cause and extent of a Security Incident.
   8.14. **"Legal Consultation Expenses"** means fees and expenses incurred by Customer to obtain data security-related legal advice after a Security Incident, including, without limitation advice related to notification content and requirements. Legal Consultation Expenses do not include any fees or expenses incurred in connection with the response to or defense of any actual, anticipated or threatened suit, action, proceeding, litigation or Compliance Action against the Customer.
   8.15. **"Measured Security Posture"** means the configurations, settings, actions and remediations described in the then-current Falcon Complete Operating Model guide as "measured".
   8.16. **"Personnel"** means Customer's employees, vendors and contractors.
   8.17. **"Physical Event"** means fire, smoke, explosion, lightning, wind, water, flood, earthquake, volcanic eruption, tidal wave, landslide, hail, an act of God, loss or theft of a physical Endpoint, or any other physical event, however caused.
   8.18. **"Post-Security Incident Expenses"** means fees and expenses incurred by Customer for (1) notifying individuals whose personally identifiable information may have been compromised by a Security Incident (including the cost

of printing and mailing) and (2) identity theft call center assistance, identity restoration services, credit file or identity monitoring and/or victim expense reimbursement insurance made available to such notified individuals.

8.19. **"Pre-existing Incident"** means any unauthorized access to the operating system of an Endpoint that occurs either (1) before such Endpoint becomes a Covered Endpoint in the Protected Environment; or (2) before Customer's Initial Warranty Period.

8.20. **"Protected Environment"** means Customer's Covered Endpoints that are in the Measured Security Posture (or higher) and monitored by the CrowdStrike's Falcon Complete Team.

8.21. **"Public Relations Expenses"** means fees and expenses incurred by Customer for a public relations firm to advise the Customer on minimizing the harm to Customer and restoring public confidence in Customer after a Security Incident.

8.22. **"Related Security Incident"** means, collectively, the same, continuous, related or repeated Pre-existing Incidents and/or Security Incidents.

8.23. **"Security Incident"** means unauthorized access by a Third Party to the operating system of a Covered Endpoint in the Protected Environment that results in the malicious exfiltration, destruction and/or irreversible encryption of Customer data that Customer reasonably believes has value in excess of $5,000. Notwithstanding the foregoing, unauthorized access arising out of or resulting directly or indirectly from any of the following events does not constitute a Security Incident: (a) Customer whitelisting a Covered Endpoint or process; (b) Customer altering or instructing CrowdStrike to alter configurations such that a Covered Endpoint falls below the Measured Security Posture; (c) Customer's failure to follow CrowdStrike's prevention or remediation instructions; (d) Customer's modification or alteration of Falcon Complete; (e) any fraudulent, criminal or malicious act of Customer or its Personnel, or any intentional or knowing violation of the law by Customer or its Personnel; (f) any Physical Event and/or (g) any form of Unrest.

8.24. **"Third Party"** means any entity or person except Customer and Personnel.

8.25. **"Unrest"** means strike or similar labor action, war, invasion, military action (whether war is declared or not), civil war, mutiny, popular or military uprising, insurrection, rebellion, revolution, military or usurped power, or any action taken to hinder or defend against any of these events.

8.26. **"Warranty Period"** means the Initial Warranty Period or a Renewal Warranty Period (both defined in Section 7.3), as applicable.

BY THE SIGNATURES BELOW THIS WARRANTY AGREEMENT IS AGREED TO AS OF THE WARRANTY EFFECTIVE DATE:

CROWDSTRIKE SERVICES, INC.		**CUSTOMER:** (Provide complete legal entity name)	
By:	Mike Forman	By:	
Name:	**Mike Forman**	Name:	
Title:	**V.P. Corporate Controller**	Title:	
Date:		Date:	
Address	150 Mathilda Place, Third Floor Sunnyvale, CA 94086	Address:	

CROWDSTRIKE

COMPROMISE ASSESSMENT

CROWDSTRIKE SERVICES

COLLECT. ANALYZE. KNOW.

Extensive experience with large and complex incident response (IR) investigations involving targeted threats allows the CrowdStrike ® Services team to offer unique insights into the tactics, techniques, and procedures (TTPs) leveraged by today's most skilled adversaries.

This knowledge and expertise combines with the CrowdStrike Falcon® platform's award-winning, cloud-delivered endpoint technology, to enable comprehensive compromise assessment of your organization's IT environment, answering the critical question, "Has my organization been breached?"

CrowdStrike Services goes far beyond traditional indicator-based detections and point-in-time monitoring: CrowdStrike's Compromise Assessment emphasizes both expert analysis of historical forensic evidence and real-time threat detection and hunting. Knowing what has happened in the past and what is happening now on your endpoints is key to understanding how to defend your cyber environment in the future.

CROWDSTRIKE METHODOLOGY AND APPROACH

A CrowdStrike Compromise Assessment begins with the efficient collection and analysis of forensic artifacts from Microsoft Windows, Mac OS X, and many Linux-based operating systems — without the need for on-premises appliances or active indicator sweeping. In parallel, the CrowdStrike Falcon platform provides real-time threat detection and monitoring of your environment, looking for both malware and malware-free threats, along with indicators of attack (IOAs), which are often indicative of active malicious "hands-on-keyboard" activity.

A true assessment of whether malicious activity has taken place within your environment can't begin without comprehensive, historical, forensics-based context, combined with dynamic monitoring. Every environment is unique, so CrowdStrike Services quickly and efficiently collaborates with your team to learn your network topology and what systems comprise your environment. With this knowledge, the team can understand and leverage the applications

ACTIONABLE ANALYSIS AND FINDINGS

CrowdStrike recognizes that for any compromise assessment to be successful, the findings and analysis reports must be actionable and appropriate for all the key stakeholders in IT security and enterprise risk management functions. Documentation provided by CrowdStrike consultants can include:

- **A presentation covering the summary findings of whether evidence of a targeted intrusion of your environment was discovered, coupled with custom recommendations for effective improvements to your security posture**
- **A written executive summary intended to capture the most significant findings, conclusions, and recommendations**
- **Technical documentation of the CrowdStrike team's assessment, intended to provide your technical team with the information they need to remediate, remove, and validate the CrowdStrike team's findings**
- **Additional discovery documentation of commodity malware, suspicious scripts and files, remote access utilities, and administration practices that introduce significant risk**

and tools used within your organization. This crucial relationship allows CrowdStrike to identify normal activity and provide you with a forensics collection, network monitoring, and endpoint detection and response (EDR) effort that is unrivaled in the cybersecurity services industry.

AWARD-WINNING TECHNOLOGY PROVIDES VISIBILITY FAST

The Compromise Assessment is conducted by CrowdStrike consultants using the following:

- **Falcon Insight ™** is CrowdStrike's endpoint detection and response (EDR) solution, offering advanced cloud-native protection in a single, lightweight agent deployed to each endpoint in your environment
- **Falcon Forensics Collector (FFC)** is a cross-platform, non-persistent, single-run tool that is deployed remotely and collects data from more than 45 forensically significant artifacts on each endpoint
- **Forensic metadata** collected by FFC, then aggregated and processed in the CrowdStrike cloud where it can be analyzed and cross-referenced against CrowdStrike Falcon Intelligence™, the cyber threat intelligence offering that tracks and identifies adversary TTPs

CrowdStrike consultants investigate the collected data for IOAs; identify statistical anomalies (e.g. suspicious patterns of process execution within your environment as a whole); track and trace evidence of lateral movement and suspicious user behavior; and highlight known malware and hacking tools.

The CrowdStrike Falcon platform provides real-time, forward-looking visibility to continuously monitor for patterns of attacker tradecraft. Malicious activities such as privilege escalation, lateral movement, malware deployment, and credential dumping can all be detected immediately, allowing you to prevent further attacker activity from compromising your endpoints.

When even greater visibility is required, CrowdStrike can provide Falcon Network Sensor technology to monitor your network ingress/egress points and identify potential malicious communications in-flight. The Falcon Network Sensor is a stealth technology that passively captures, analyzes, and dissects network traffic, leveraging CrowdStrike Falcon Intelligence and custom detection patterns to alert on suspicious communications. Just as with FFC and Falcon platform data, the Falcon Network Sensor telemetry is aggregated within the CrowdStrike cloud infrastructure and analyzed by the CrowdStrike team of experienced network security monitoring (NSM) hunters.

LEARN HOW CROWDSTRIKE STOPS BREACHES:

VISIT WWW.CROWDSTRIKE.COM/SERVICES

Speak to a representative to learn more about how CrowdStrike Services can help you prepare for and defend against targeted attacks.

LET'S DISCUSS YOUR NEEDS

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/services

CROWDSTRIKE

CROWDSTRIKE FALCON DEVICE CONTROL

Ensures safe device usage, extensive visibility and granular control: the industry's only cloud-delivered device control solution

CROWDSTRIKE FALCON DEVICE CONTROL

ENSURING SAFE AND ACCOUNTABLE DEVICE USAGE

The portability and usability of USB devices make them essential in today's enterprise environments. Yet these devices pose a significant security risk, bringing malware into organizations and leaking data out. Although device control solutions exist, they don't provide the contextual visibility and granular control required to understand and manage today's powerful devices.

Falcon Device Control™ ensures the safe utilization of USB devices across your organization. Built on the Falcon platform, it uniquely combines extensive visibility and granular control, allowing administrators to ensure that only approved devices are used in your environment. It also provides real-time and historical visibility, including detailed logging and reporting capabilities, giving you a complete understanding of device usage and files written to devices.

Leveraging the power of the CrowdStrike® platform and accessed through the Falcon management console, Falcon Device Control is the industry's only 100 percent cloud-delivered and managed device control solution.

KEY BENEFITS

- Mitigate risks associated with USB devices
- Gain automatic and complete visibility on USB device usage
- Control device usage with precision
- Implement and manage policies without hassle

KEY PRODUCT CAPABILITIES

UNPRECEDENTED VISIBILITY ACROSS USB DEVICE USAGE — EFFORTLESSLY

Discover devices automatically
Gain continuous insight into USB devices across your organization, including those not covered by a policy. Falcon Device Control automatically reports device type (e.g. mass storage, human interface, etc.) with manufacturer, product name, and serial number. You have visibility into all devices operating over the USB bus, including internal/non-removable USB devices and those not categorized as USB by Windows, such as Bluetooth.

A wealth of information at your fingertips
Immediately see which devices are used in your environment and how they are being used at a glance via usage dashboards. Falcon Device Control provides insight into specific files copied to a removable drive, processes executed from USB storage, users, and hosts where USB devices were used.

Immediate and powerful search capabilities
Falcon Device Control provides fast and powerful real-time and historical search capabilities. Examine your environment for vital information such as the devices used on a specific machine and file writes to mass storage.

PRECISE AND GRANULAR POLICY ENFORCEMENT

Strict policy enforcement
Define device control policies for endpoint groups, whitelist and blacklist devices by class, vendor, product serial number and/or specific device ID. Define device control policies for endpoints both on and offline.

See the impact of policies before implementing them
Alerts and dashboards allow you to see how your policies will impact users before rolling them out.

Define granular policies for drives
Allows read/write or read-only access, while blocking execution of applications on USB drives.

Monitor files written to storage
Track data moving from your endpoints to storage, giving you visibility into what's being copied to devices.

Automatically get device information for quick and easy policy creation and management workflows
Falcon Device Control automatically obtains devices' vendor, class model and serial number, without requiring the use of external tools or device managers, allowing you to create policies for all devices being used in your environment.

Allows devices to charge even when access is denied
Charge your USB devices while simultaneously enforcing your device control policies.

SEAMLESS INTEGRATION WITH FALCON ENDPOINT PROTECTION

One agent, one console, one platform
As a 100 percent cloud managed and delivered solution, Falcon Device Control is enabled via the same lightweight Falcon agent, managed by the same console, and fully integrated with the Falcon platform.

Immediate implementation and management
Falcon Device Control hits the ground running and is operational in minutes.

EMPOWERS YOU WITH IMMEDIATE USB DEVICE VISIBILITY AND PROTECTION AT YOUR FINGERTIPS

You want your users to be able to use their portable devices without being exposed to the inherent risks. That's why Falcon Device Control provides the granular visibility and control needed to enable safe device usage, while leveraging the extensibility of the Falcon platform.

UNPARALLELED VISIBILITY AND GRANULAR CONTROL

Falcon Device Control provides unparalleled visibility over USB device usage and granular control over utilization, for fast and easy mitigation of the risks associated with those devices.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

CROWDSTRIKE

Falcon Endpoint Protection - COMPLETE

Operating Model

Table of Contents

OVERVIEW

CrowdStrike Falcon Endpoint Protection (EPP) Complete™ is a capability built on the CrowdStrike Falcon Platform. Customers gain market leading endpoint protection by combining Falcon Prevent (NGAV), Falcon Insight (EDR) and Falcon OverWatch (managed threat hunting). Additionally, the Falcon Endpoint Protection Team (EPP Team) manages and actively monitors the Falcon platform for you and remotely remediates incidents as needed. The CrowdStrike Falcon EPP Complete solution combines the effectiveness of the CrowdStrike Falcon platform with the efficiency of a dedicated team of CrowdStrike security professionals, executing focused

incident handling playbooks.

We will work together to apply different playbook postures to the various asset groups you identify in your environment. We will configure sensor grouping and apply prevention postures to put your security strategy into action.

This document will establish the standard operating procedures and describe how the EPP Protection Team will work to manage the Falcon platform as well as respond to the various types of detections that the platform may generate.

PLAYBOOK SECURITY POSTURES

There are three Playbook Security Postures used by the EPP Team: Active Posture, Measured Posture, and Cautious Posture.

Each Playbook Security Posture determines how the Falcon Platform and the EPP Team handles a system in your environment.

Playbook Security Postures define two things:

1. The EPP Team configuration of the Falcon Platform prevention policies.
2. The countermeasures the EPP Team is pre-approved to use in remediating a system.

Playbook Posture Descriptions

Cautious:
Systems in Cautious Posture will have a lower risk of disruption by Falcon and the EPP Team but also a higher risk of compromise by malicious activity that does not have a high confidence detection. In this posture, remediation will take longer as countermeasures that are not pre-approved will need to be escalated to you for approval.

Highlights:

- Only non-disruptive remediation countermeasures are pre-approved.
- NGAV Prevention Policy set to prevent only High Severity detections.

Measured:
Systems in Measured Posture take a middle of the road approach allowing higher preventions from Falcon and all but inherently disruptive countermeasures as pre-approved. This allows for immediate prevention of potentially malicious activity that may not be prevented under Cautious Posture and allows for rapid remediation of compromised systems by the EPP Team. Lower confidence detections will not be prevented under this posture.

Highlights:

- Inherently disruptive Countermeasures not pre-approved (Reboot/Network Isolation).

- NGAV Prevention Policy set to prevent only Critical, High, and Medium severity detections.

Active:
Systems in Active Posture have the highest level of Falcon prevention and pre-approve the EPP Team to take any of the listed countermeasures required to remediate a system. Active Posture will mitigate the most amount of risk from malicious activity but may also cause an increase in false positive detections. These false positives will be identified and whitelisted on a case by case basis.

Highlights:
- All EPP Team Countermeasures pre-approved to remediate a compromised system.
- NGAV Prevention Policy set to prevent all levels of severity detections.

PLAYBOOK SECURITY POSTURES DETAILS

Windows - Falcon Platform Policy Configuration

Type	Category		Cautious Posture	Measured Posture	Active Posture
Sensor Capability	End User Notifications		Disabled	Disabled	Disabled
Sensor Visibility	Enhanced Visibility	Additional User Mode Data	Enabled	Enabled	Enabled
		Interpreter-Only	Enabled	Enabled	Enabled
		Engine (Full Visibility)	Disabled	Disabled	Enabled
Next-Gen Antivirus	Cloud Machine Learning	Cloud Anti-Malware Detection	Moderate	Aggressive	Aggressive
		Cloud Anti-Malware Prevention	Cautious	Moderate	Aggressive
		Adware/Pup Detection	Cautious	Moderate	Aggressive
		Adware/Pup Prevention	Cautious	Moderate	Aggressive
	Sensor Machine Learning	Sensor Anti-Malware Detection	Moderate	Aggressive	Aggressive
		Sensor Anti-Malware Prevention	Cautious	Moderate	Aggressive
	Quarantine	Quarantine & Security Center Registration	Enabled	Enabled	Enabled

Malware Protection	Execution Blocking	Custom Blacklisting	Disabled	Enabled	Enabled
		Prevent Suspicious Processes	Disabled	Enabled	Enabled
		Malicious PowerShell Scripts or Commands	Disabled	Enabled	Enabled
Behavior-Based Prevention	Exploit Mitigation Prevention	Force ASLR	Disabled	Disabled	Disabled
		Force DEP	Disabled	Disabled	Disabled
		Heap Spray Preallocation	Disabled	Enabled	Enabled
		NULL Page Allocation	Disabled	Disabled	Enabled
		SEH Overwrite Protection	Disabled	Disabled	Enabled
		Untrusted Font Loading	Disabled	Disabled	Enabled
		Remote Library Loading	Disabled	Disabled	Enabled
	Ransomware Prevention	Backup Deletion	Enabled	Enabled	Enabled
		Cryptowall	Enabled	Enabled	Enabled
		Ransomware File Extension	Enabled	Enabled	Enabled
		Locky	Enabled	Enabled	Enabled
		File System Access	Disabled	Disabled	Enabled
	Exploitation Behavior Prevention IOAs	Application Exploitation Activity	Disabled	Enabled	Enabled
		Chopper Webshell	Disabled	Enabled	Enabled
		Drive-by-Download	Disabled	Enabled	Enabled
		JavaScript Execution via Rundll32	Disabled	Enabled	Enabled
	Lateral Movement IOAs	Windows Logon Bypass Prevention	Enabled	Enabled	Enabled

Mac - Falcon Platform Prevention Policy Configuration

Type	Category		Cautious Posture	Measured Posture	Active Posture
Next-Gen Antivirus	Cloud Machine Learning	Cloud Anti-Malware Detection	Moderate	Aggressive	Aggressive
		Cloud Anti-Malware Prevention	Cautious	Moderate	Aggressive
		Adware & PUP Detection	Cautious	Moderate	Aggressive
		Adware & PUP Prevention	Cautious	Moderate	Aggressive
	Quarantine	Quarantine	Enabled	Enabled	Enabled
Malware Protection	Execution Blocking	Custom Blacklisting	Disabled	Enabled	Enabled
		Prevent Suspicious Processes	Disabled	Enabled	Enabled
Behavior-Based Prevention	Unauthorized Remote Access IOAs	XPCOM Shell	Disabled	Enabled	Enabled
		Chopper Webshell	Disabled	Enabled	Enabled
		Empyre Backdoor	Disabled	Enabled	Enabled
	Credential Dumping IOAs	KcPassword Decoded	Disabled	Enabled	Enabled
		Hash Collector	Disabled	Enabled	Enabled

ASSET GROUPS

Asset Groups allow you to organize systems into groups and apply one of the three security postures to each group.[1]

This allows flexibility in how the EPP Team approaches different systems in your environment and how aggressive the Falcon Platform is configured to prevent potentially malicious activity.

Multiple Asset Groups are optional as you can choose to place all your assets in one group with one Playbook Posture applied or break down your assets in the Asset Group sheet in **Appendix B**. An example Asset Group assignment is shown below.

Criteria for assigning assets to a group will be defined in Appendix B.

Asset Group	Playbook Posture	Assignment Criteria
Workstations	Active Posture	OS Type
Servers	Measured Posture	OS Type
Critical Servers	Cautious Posture	CSV List
VIP Workstations	Measured Posture	CSV List

[1] The EPP Complete Warranty is valid only under Measured and Active Postures.

COUNTERMEASURES

During the course of incident handling, the EPP Team may need to take remediation actions. In accordance with this operating model, the table below describes at a high level what types of countermeasures are preapproved in each posture. When the EPP Team needs to implement countermeasures that are not preapproved, an escalation will be sent to you for approval.

Windows/macOS – EPP Complete Countermeasures

Analyst Countermeasure	Windows/macOS Cautious	Windows/macOS Measured	Windows/macOS Active
Quarantine File	x	x	x
Pull File for Analysis	x	x	x
Event Log Review	x	x	x
Global Process Hash Block		x	x
End Process		x	x
Stop Service		x	x
Disable Registry/PLIST Persistence		x	x
Isolate System		*	x
Restart System			x

*** System Isolation will still only be implemented for systems in Measured Posture in cases of data exfiltration or spreading ransomware.**

Linux – EPP Complete Countermeasures

Analyst Countermeasure	Linux Cautious	Linux Moderate*	Linux Agile*
Quarantine File	x	x	x
Pull File for Analysis	x	x	x
Event Log Review	x	x	x
Global Process Hash Block		x	x
End Process		x	x
Stop Service		x	x
Disable PLIST Persistence		x	x
Restart System			x

***Measured/Active Definitions are reserved for Windows/macOS systems because at this time we do not provide NGAV on Linux systems.**

COMMUNICATIONS

System Remediated Notification

At the conclusion of each handled incident, the EPP Team will send a summary report outlining what was observed, what actions were taken, and any required next steps. The notification will include the data elements shown in the following example.

Incident Details

System_Hostname:
JoePC

Username:
Administrator

System_IP_Address:
192.168.10.106

Detection_Scenario:
Known Malware - Ursnif

Detection_Severity:
HIGH

Detection_Details:
https://falcon.crowdstrike.com/activity/detections...

Date_of_Initial_Compromise:
20180611

Analysis_and_Remediation_Details:
The user fell victim to a phish which led to the installation of Ursnif malware.

Processes Stopped:
Markerscaler.exe

Quarantined Files:
C:\Users\Administrator\Downloads\Emails Models.docx
C:\Users\ Administrator\AppData\Local\Temp\67406.exe
C:\ProgramData\KdbNNb.exe
C:\Users\ Administrator\AppData\Local\Temp\ouxlfcbtocvpzpvhvgtsafmfds.txt
C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\exhphlda.miy
C:\Users\Administrator\AppData\local\Microsoft\Doetduo.wpq
C:\windows\SysWOW64\g3IhVX8KQNMnRx.exe

Removed Regkey's
HKCU\Software\Microsoft\Windows\Currentversion\Run
ychfmxl REG_SZ C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe "$windowsupdate =
\"C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe\"; & $windowsupdate"

Removed Scheduled Tasks related to the malware
125275F5-F470-4919-9A18-234F29DAB5C4
cmd.exe /C "start /MIN C:\windows\system32\cscript.exe //E:javascript "C:\Users\Administrator\AppData\Local\Microsoft\doetdu.wpq""

Recommended_Recovery_Tasks:
Reset Administrator password

Escalations

Escalations will be sent via email when the EPP Team requires action from you in order to remediate a system. Not having remote access to a system, needing approval to take additional remediation countermeasures, and recommendations to rebuild a system that has been irreparably damaged are examples of when an escalation will be sent via email.

The key difference between a System Remediated Notification and an Escalation is that Escalations require your action before the EPP Team can move forward with triage or remediation whereas System Remediated Notifications are those situations where the EPP Team has remediated a system(s) and is providing post-incident details of the actions taken to remediate the system(s).

Critical Escalations

When an escalation is required for a critical severity detection, the EPP Team will utilize the call roster provided by you in Appendix B to notify you.

Critical incidents are those incidents that involve:

- Destructive malware that was not blocked
- Interactive, hands on keyboard attacker
- Apparent theft of sensitive data (i.e. IP theft or PCI data)

During critical incident handling where remediation actions require approval or action needs to be taken by you during an incident, the EPP Team will attempt to call the phone numbers provided in Appendix B in order of priority. If there is no response from any of the contacts, the EPP Team will send a Critical Escalation email and continue monitoring but not proceed with any unapproved countermeasures.

In Appendix B, you will provide a contact list in order of priority when escalation is required.

METRICS

On a monthly basis, you will get an executive metrics dashboard that highlights the overall state of endpoint security in your environment, trended month over month. We will provide high level aggregate statistics that describe the performance of the solution covering two main areas.

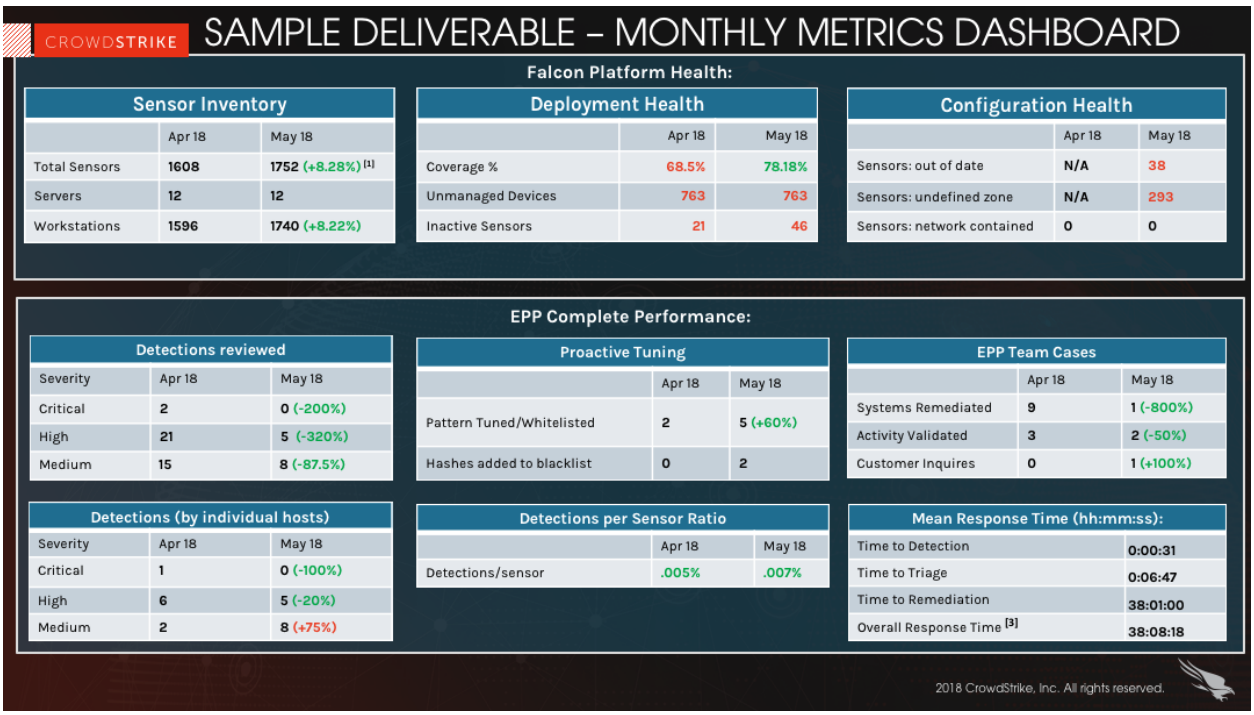
Falcon Platform Health:

- Information about the inventory of the sensor deployment
- Coverage information describing our understanding of the relative amount of the environment we believe to have deployed
- Information about the health of the sensors themselves, with respect to version management and prevention policy application

EPP Team Performance:

- Number of detections triaged by the team, also broken down by hosts
- Effort associated with improving the quality of detections in your environment through whitelisting and tuning of detections patterns
- Number and types of incidents and cases worked by the team
- Metrics about the speed of our response to detections we observe

Example monthly metrics dashboard:



CROWDSTRIKE SAMPLE DELIVERABLE – MONTHLY METRICS DASHBOARD

Falcon Platform Health:

Sensor Inventory	Apr 18	May 18
Total Sensors	1608	1752 (+8.28%) [1]
Servers	12	12
Workstations	1596	1740 (+8.22%)

Deployment Health	Apr 18	May 18
Coverage %	68.5%	78.18%
Unmanaged Devices	763	763
Inactive Sensors	21	46

Configuration Health	Apr 18	May 18
Sensors: out of date	N/A	38
Sensors: undefined zone	N/A	293
Sensors: network contained	0	0

EPP Complete Performance:

Detections reviewed		
Severity	Apr 18	May 18
Critical	2	0 (-200%)
High	21	5 (-320%)
Medium	15	8 (-87.5%)

Proactive Tuning	Apr 18	May 18
Pattern Tuned/Whitelisted	2	5 (+60%)
Hashes added to blacklist	0	2

EPP Team Cases	Apr 18	May 18
Systems Remediated	9	1 (-800%)
Activity Validated	3	2 (-50%)
Customer Inquires	0	1 (+100%)

Detections (by individual hosts)		
Severity	Apr 18	May 18
Critical	1	0 (-100%)
High	6	5 (-20%)
Medium	2	8 (+75%)

Detections per Sensor Ratio	Apr 18	May 18
Detections/sensor	.005%	.007%

Mean Response Time (hh:mm:ss):	
Time to Detection	0:00:31
Time to Triage	0:06:47
Time to Remediation	38:01:00
Overall Response Time [3]	38:08:18

SENSOR UPDATE POLICIES

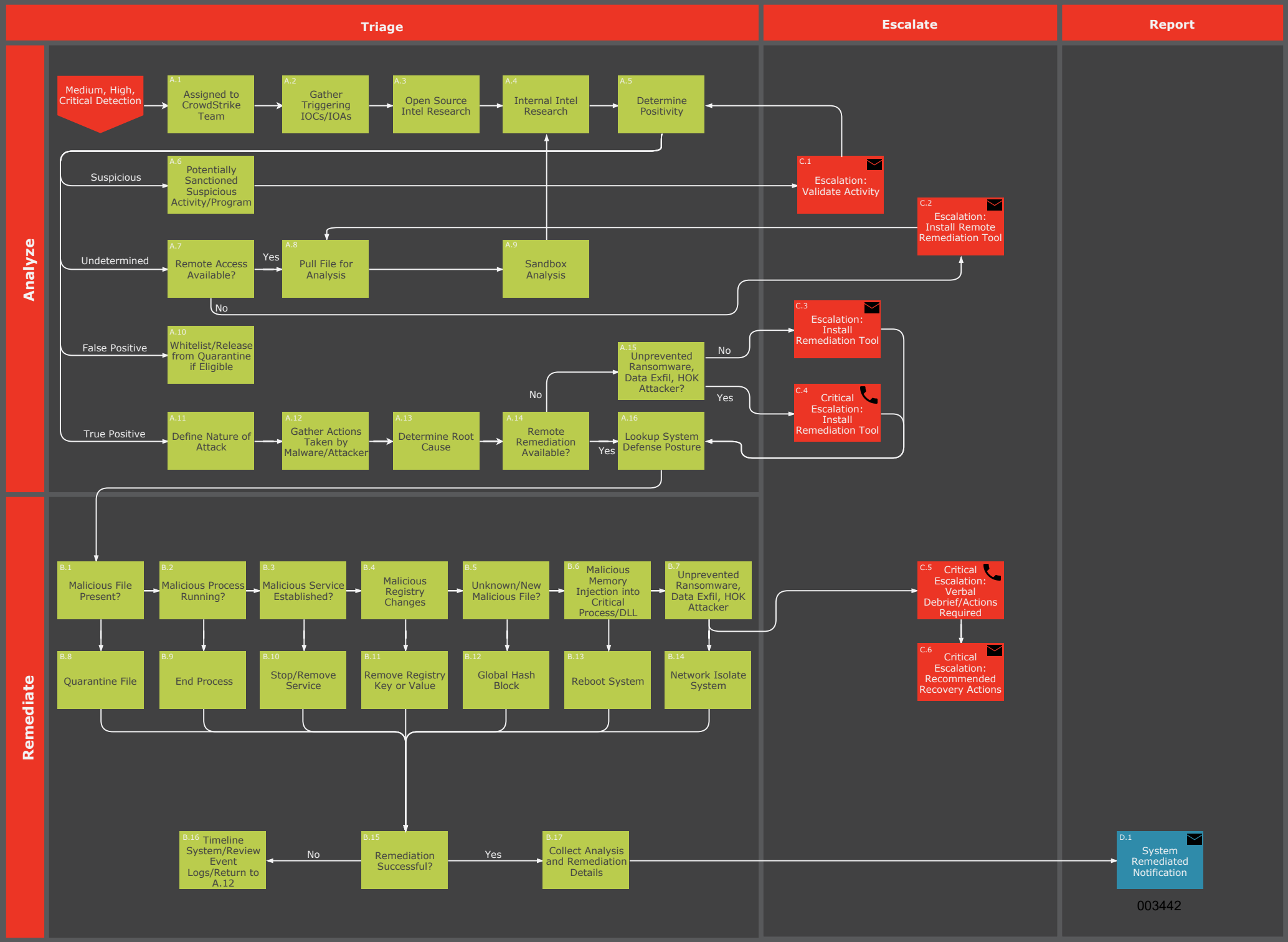
A Sensor Update Policy will be specified for each Asset Group in **Appendix B**.

This tells the EPP Team when you would like sensors upgraded as new versions are released and gives you the option and flexibility to roll out updates to different systems on a deferment schedule. The EPP Team will update sensors per asset group on your behalf according to the deferment set in Appendix B unless a problem is identified in which case the update may be placed on hold until resolved.

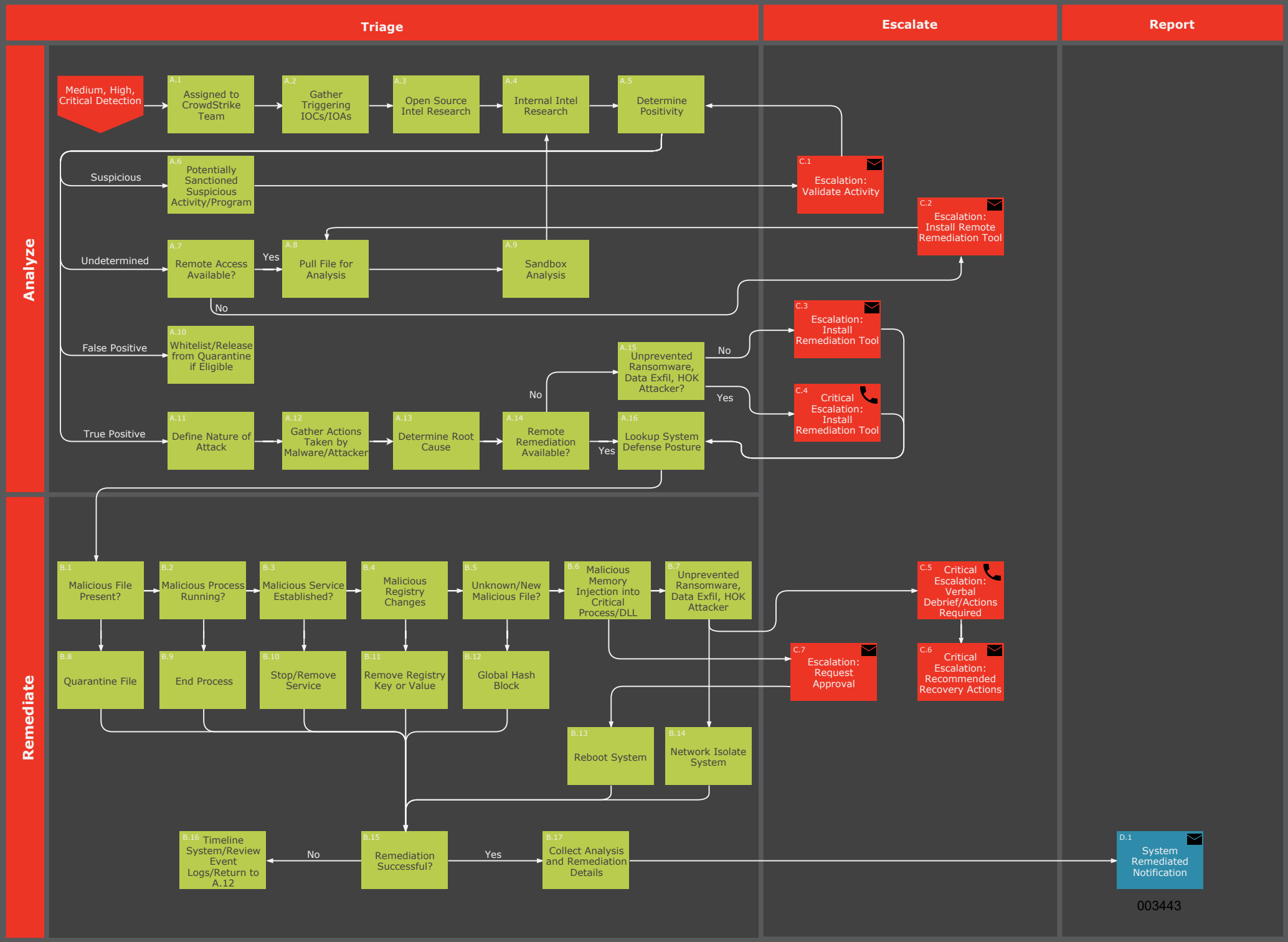
Updates can be set to Auto or on a weekly deferment of up to eight weeks.

EPP INCIDENT HANDLING WORKFLOWS

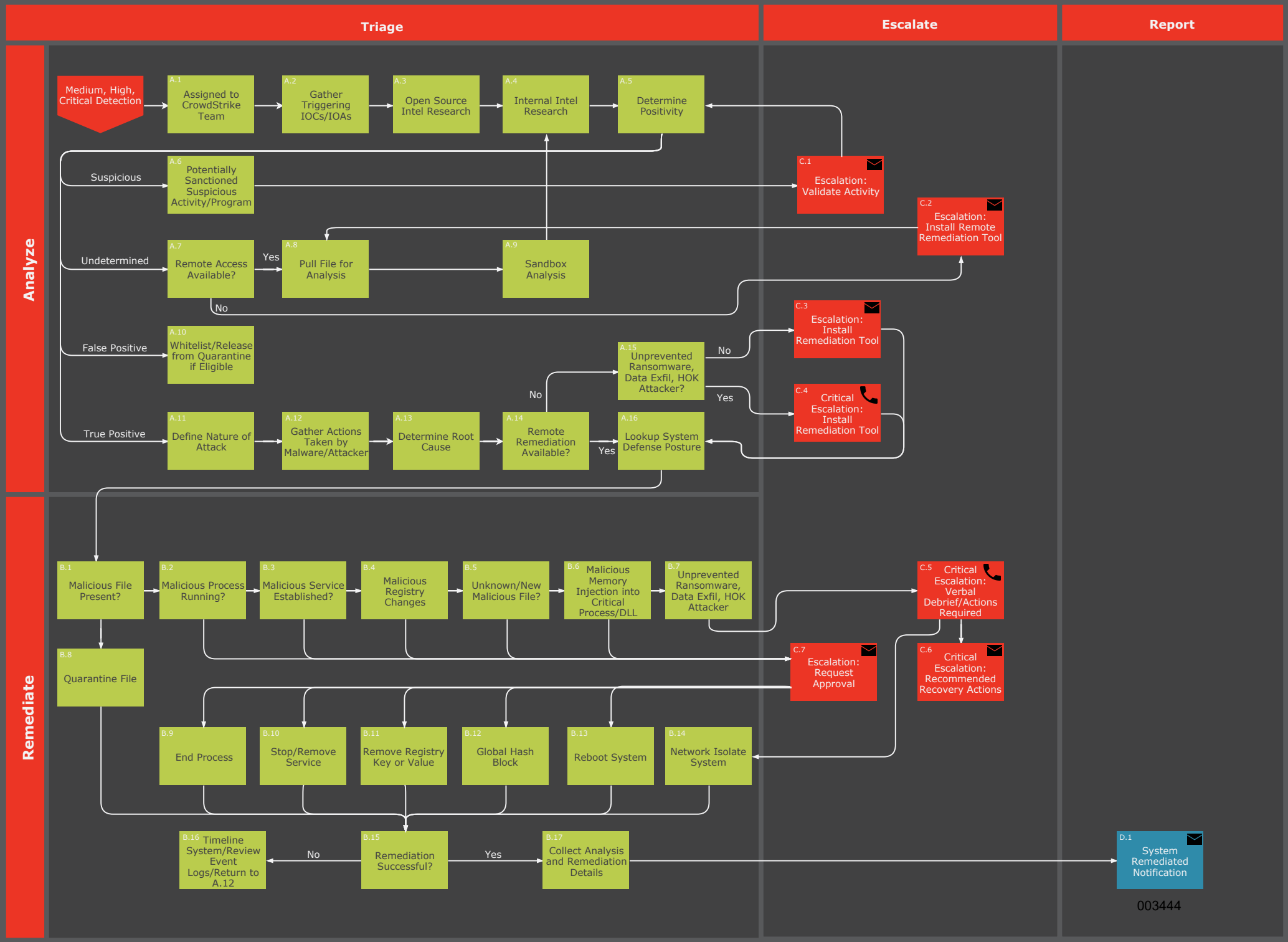
Playbook: Active Posture - EPP Complete



Playbook: Measured Posture - EPP Complete



Playbook: Cautious Posture - EPP Complete



COUNTERMEASURES EXPLAINED

Quarantine File

Suspected malicious files may be quarantined in place to prevent, cease, or remove a threat to a system or network. Quarantined files will typically be kept in an encrypted state on the host in the chance that the file needs to be restored.

Pull File for Analysis

On occasion, analysts may copy a suspected malicious file from a system for analysis to confirm if there is malicious behavior, code, or intent in the file. This will be done only when the malicious nature of a file is not certain and where hash blocking or quarantining the file without this analysis has the potential to disrupt.

Event Log Review

On occasion, analysts may conduct system forensics to include event log reviews, network analysis, file forensics, and registry reviews in order to confirm, contain, remediate, or eradicate malicious files or threat actors on a system.

End Process

On occasion, analysts may end a suspected malicious process in order to contain, remediate, or eradicate malware or a threat actor on a system.

Stop Service

On occasion, analysts may end a suspected malicious service in order to contain, remediate, or eradicate malware or a threat actor on a system.

Remove Registry Persistence

On occasion, analysts may remove a malicious registry object in order to contain, remediate, or eradicate malware or a threat actor on a system.

Global Process Hash Block

Processes identified as malicious may be placed into the process hash block list unique to your organization. This will block that processes hash across any system with the process hash blocking prevention enabled on the Falcon Platform Sensor.

Isolate System

On occasion, systems identified as dangerous to the network, to other systems, with potential C2 communications occurring, or with data exfiltration of potentially sensitive data may be placed in network isolation. Communications with the Falcon Platform will remain established but communication with other systems will not be allowed until taken out of isolation.

Restart System

On occasion, analysts may need to reboot a system to effectively remediate a compromise or infection.

OPERATIONS OVERVIEW

The EPP Team provides Falcon Platform management and managed threat response on a 24x7 basis. CrowdStrike will work with you to develop this document and its appendices as the mutually agreed upon method of operations. The EPP Operating Model will cover those endpoints on which the Falcon sensor has been installed and on boarded to one of the Playbook Security Postures ("Covered Endpoints"). In the event of a Falcon Platform detection, the EPP Team will act in accordance with the EPP Operating Model. The parties will mutually agree in the EPP Operating Model on the method for remediation, if any. The EPP Team will not perform remediation tasks that fall outside the scope of the countermeasures listed and as described within the EPP Operating Model.

The EPP Team does not perform: (i) forensic disk analysis, (ii) other advisory or consulting services, such as, but not limited to, systems configuration management, patch management, user awareness training, penetration testing, (iii) other strategic cyber security services, (iv) data recovery services for deleted, encrypted or otherwise lost data; or (iv) any services for any systems or endpoints other than Covered Endpoints.

Falcon Platform technical support addressing engineering issues with detections, platform performance, or platform function will be directed to CrowdStrike Support.

TRIAGE OVERVIEW

The EPP Team will triage Falcon detections according to the EPP Team Incident Handling Flowchart. Detections that are Medium, High, or Critical will be triaged for those systems that are Covered Endpoints.

Low detections are used by the EPP Team as additional information during an incident and will typically not be triaged on their own unless accompanied by a higher severity detection.

Duplicate detections or multiple detections on the same system that are identified by the EPP Team as part of one incident will often be grouped and triaged under one detection. This singular detection will reflect the assignment and status of EPP Team's work on that detection in the Falcon dashboard. The other related detections to the incident in the Falcon dashboard may be marked as ignored due to this grouping but are still being triaged, analyzed, and, where needed, responded to according to the Operating Model.

NEXT STEPS

Due From	Action Item	Due
You	Fill out Appendix B: Playbooks	Post onboarding call
You	Deploy ConnectWise globally	Until complete
You	Deploy Falcon globally	Until complete
CrowdStrike	Implement Asset Groups and Prevention Policies	After Receiving Completed Appendix B
CrowdStrike	Begin Managing Falcon Platform, Monitoring & Triaging Detections, and Remediating Systems	After Implementing Asset Groups and Prevention Policies

APPENDIX A: DATA ACCESS AND EVIDENCE HANDLING

Remote Remediation

Method

A lightweight agent, ConnectWise Control, is installed on each covered endpoint to facilitate remote remediation. ConnectWise Control is a secure cloud based remote access solution that provides remote remediation capabilities to the EPP Team.

Limited Access

The only employees of CrowdStrike that have access to the ConnectWise system are members of the EPP Team. EPP Team employees are residents of the USA, UK, or Australia. All members of the EPP Team are vetted through a background check prior to employment.

Access Controls

The EPP Team will access covered systems via TLS encryption and Multi-Factor Authentication (MFA). Each analyst account is authorized via password and second factor rotating key. ConnectWise allows for Role Based Access Control (RBAC) and the access performed by each account are tied to a specific analyst by name. Members of the EPP Team will only access systems for the purpose of incident triage or remediation. Any remediation actions done by an EPP Team analyst occur as a background task on the system account and are not visible to the end user.

Audit

Logs detailing the connections made by each user account as well as remote remediation commands sent by each user account are held active for a period of thirty (30) days by CrowdStrike. Any time EPP analysts take actions in a customer environment, a FLASH Notification will be sent outlining actions performed in coordination with a remediation event.

Monitoring and Segregation of Duties

In addition to access restriction controls and audit controls, every endpoint that has the ConnectWise agent on it also has the Falcon agent installed on it. Activities performed by the EPP Team will result in data that is observed by the Falcon agent. Activities associated with remediation tasks will be viewable by customers via the Falcon Insight module, and will also be hunted by OverWatch analysts, to create a high level of visibility into remediation tasks.

Evidence Handling

Throughout the course of an incident, further analysis may need to be conducted on select files from a covered system. This data is typically malware samples, event logs, or filesystem artifacts, and is rarely any user created binary content such as office documents. Any data collected for further analysis will be encrypted in transit and encrypted at rest. The EPP Team will utilize a secure file copy process to extract those select files from the system. Files of interest may include suspected malicious documents, suspected malicious binaries, files

potentially related to those malicious documents and binaries, and system event logs that may contain additional data points required to fully remediate a covered system.
Secure File Transfer Protocol (SFTP) is utilized to transfer files to a secure internal CrowdStrike Services forensics lab directory to which only the EPP Team has access. A write only SFTP account will be utilized to deliver files of interest selected by an analyst to the CrowdStrike forensics lab.
CrowdStrike does not retain any customer collected data for longer than necessary to conduct analysis and remediate an incident. Any collected evidence will not be shared outside of CrowdStrike.

CROWDSTRIKE

Falcon Endpoint Protection - COMPLETE

Operating Model

Table of Contents

OVERVIEW

CrowdStrike Falcon Endpoint Protection (EPP) Complete™ is a capability built on the CrowdStrike Falcon Platform. Customers gain market leading endpoint protection by combining Falcon Prevent (NGAV), Falcon Insight (EDR) and Falcon OverWatch (managed threat hunting). Additionally, the Falcon Endpoint Protection Team (EPP Team) manages and actively monitors the Falcon platform for you and remotely remediates incidents as needed. The CrowdStrike Falcon EPP Complete solution combines the effectiveness of the CrowdStrike Falcon platform with the efficiency of a dedicated team of CrowdStrike security professionals, executing focused

incident handling playbooks.

We will work together to apply different playbook postures to the various asset groups you identify in your environment. We will configure sensor grouping and apply prevention postures to put your security strategy into action.

This document will establish the standard operating procedures and describe how the EPP Protection Team will work to manage the Falcon platform as well as respond to the various types of detections that the platform may generate.

PLAYBOOK SECURITY POSTURES

There are three Playbook Security Postures used by the EPP Team: Active Posture, Measured Posture, and Cautious Posture.

Each Playbook Security Posture determines how the Falcon Platform and the EPP Team handles a system in your environment.

Playbook Security Postures define two things:

1. The EPP Team configuration of the Falcon Platform prevention policies.
2. The countermeasures the EPP Team is pre-approved to use in remediating a system.

Playbook Posture Descriptions

Cautious:
Systems in Cautious Posture will have a lower risk of disruption by Falcon and the EPP Team but also a higher risk of compromise by malicious activity that does not have a high confidence detection. In this posture, remediation will take longer as countermeasures that are not pre-approved will need to be escalated to you for approval.

Highlights:

- Only non-disruptive remediation countermeasures are pre-approved.
- NGAV Prevention Policy set to prevent only High Severity detections.

Measured:
Systems in Measured Posture take a middle of the road approach allowing higher preventions from Falcon and all but inherently disruptive countermeasures as pre-approved. This allows for immediate prevention of potentially malicious activity that may not be prevented under Cautious Posture and allows for rapid remediation of compromised systems by the EPP Team. Lower confidence detections will not be prevented under this posture.

Highlights:

- Inherently disruptive Countermeasures not pre-approved (Reboot/Network Isolation).

- NGAV Prevention Policy set to prevent only Critical, High, and Medium severity detections.

Active:
Systems in Active Posture have the highest level of Falcon prevention and pre-approve the EPP Team to take any of the listed countermeasures required to remediate a system. Active Posture will mitigate the most amount of risk from malicious activity but may also cause an increase in false positive detections. These false positives will be identified and whitelisted on a case by case basis.

Highlights:
- All EPP Team Countermeasures pre-approved to remediate a compromised system.
- NGAV Prevention Policy set to prevent all levels of severity detections.

PLAYBOOK SECURITY POSTURES DETAILS

Windows - Falcon Platform Policy Configuration

Type	Category		Cautious Posture	Measured Posture	Active Posture
Sensor Capability	End User Notifications		Disabled	Disabled	Disabled
Sensor Visibility	Enhanced Visibility	Additional User Mode Data	Enabled	Enabled	Enabled
		Interpreter-Only	Enabled	Enabled	Enabled
		Engine (Full Visibility)	Disabled	Disabled	Enabled
Next-Gen Antivirus	Cloud Machine Learning	Cloud Anti-Malware Detection	Moderate	Aggressive	Aggressive
		Cloud Anti-Malware Prevention	Cautious	Moderate	Aggressive
		Adware/Pup Detection	Cautious	Moderate	Aggressive
		Adware/Pup Prevention	Cautious	Moderate	Aggressive
	Sensor Machine Learning	Sensor Anti-Malware Detection	Moderate	Aggressive	Aggressive
		Sensor Anti-Malware Prevention	Cautious	Moderate	Aggressive
	Quarantine	Quarantine & Security Center Registration	Enabled	Enabled	Enabled

Malware Protection	Execution Blocking	Custom Blacklisting	Disabled	Enabled	Enabled
		Prevent Suspicious Processes	Disabled	Enabled	Enabled
		Malicious PowerShell Scripts or Commands	Disabled	Enabled	Enabled
Behavior-Based Prevention	Exploit Mitigation Prevention	Force ASLR	Disabled	Disabled	Disabled
		Force DEP	Disabled	Disabled	Disabled
		Heap Spray Preallocation	Disabled	Enabled	Enabled
		NULL Page Allocation	Disabled	Disabled	Enabled
		SEH Overwrite Protection	Disabled	Disabled	Enabled
		Untrusted Font Loading	Disabled	Disabled	Enabled
		Remote Library Loading	Disabled	Disabled	Enabled
	Ransomware Prevention	Backup Deletion	Enabled	Enabled	Enabled
		Cryptowall	Enabled	Enabled	Enabled
		Ransomware File Extension	Enabled	Enabled	Enabled
		Locky	Enabled	Enabled	Enabled
		File System Access	Disabled	Disabled	Enabled
	Exploitation Behavior Prevention IOAs	Application Exploitation Activity	Disabled	Enabled	Enabled
		Chopper Webshell	Disabled	Enabled	Enabled
		Drive-by-Download	Disabled	Enabled	Enabled
		JavaScript Execution via Rundll32	Disabled	Enabled	Enabled
	Lateral Movement IOAs	Windows Logon Bypass Prevention	Enabled	Enabled	Enabled

Mac - Falcon Platform Prevention Policy Configuration

Type	Category		Cautious Posture	Measured Posture	Active Posture
Next-Gen Antivirus	Cloud Machine Learning	Cloud Anti-Malware Detection	Moderate	Aggressive	Aggressive
		Cloud Anti-Malware Prevention	Cautious	Moderate	Aggressive
		Adware & PUP Detection	Cautious	Moderate	Aggressive
		Adware & PUP Prevention	Cautious	Moderate	Aggressive
	Quarantine	Quarantine	Enabled	Enabled	Enabled
Malware Protection	Execution Blocking	Custom Blacklisting	Disabled	Enabled	Enabled
		Prevent Suspicious Processes	Disabled	Enabled	Enabled
Behavior-Based Prevention	Unauthorized Remote Access IOAs	XPCOM Shell	Disabled	Enabled	Enabled
		Chopper Webshell	Disabled	Enabled	Enabled
		Empyre Backdoor	Disabled	Enabled	Enabled
	Credential Dumping IOAs	KcPassword Decoded	Disabled	Enabled	Enabled
		Hash Collector	Disabled	Enabled	Enabled

ASSET GROUPS

Asset Groups allow you to organize systems into groups and apply one of the three security postures to each group.[1]

This allows flexibility in how the EPP Team approaches different systems in your environment and how aggressive the Falcon Platform is configured to prevent potentially malicious activity.

Multiple Asset Groups are optional as you can choose to place all your assets in one group with one Playbook Posture applied or break down your assets in the Asset Group sheet in **Appendix B**. An example Asset Group assignment is shown below.

Criteria for assigning assets to a group will be defined in Appendix B.

Asset Group	Playbook Posture	Assignment Criteria
Workstations	Active Posture	OS Type
Servers	Measured Posture	OS Type
Critical Servers	Cautious Posture	CSV List
VIP Workstations	Measured Posture	CSV List

[1] The EPP Complete Warranty is valid only under Measured and Active Postures.

COUNTERMEASURES

During the course of incident handling, the EPP Team may need to take remediation actions. In accordance with this operating model, the table below describes at a high level what types of countermeasures are preapproved in each posture. When the EPP Team needs to implement countermeasures that are not preapproved, an escalation will be sent to you for approval.

Windows/macOS – EPP Complete Countermeasures

Analyst Countermeasure	Windows/macOS Cautious	Windows/macOS Measured	Windows/macOS Active
Quarantine File	x	x	x
Pull File for Analysis	x	x	x
Event Log Review	x	x	x
Global Process Hash Block		x	x
End Process		x	x
Stop Service		x	x
Disable Registry/PLIST Persistence		x	x
Isolate System		*	x
Restart System			x

*** System Isolation will still only be implemented for systems in Measured Posture in cases of data exfiltration or spreading ransomware.**

Linux – EPP Complete Countermeasures

Analyst Countermeasure	Linux Cautious	Linux Moderate*	Linux Agile*
Quarantine File	x	x	x
Pull File for Analysis	x	x	x
Event Log Review	x	x	x
Global Process Hash Block		x	x
End Process		x	x
Stop Service		x	x
Disable PLIST Persistence		x	x
Restart System			x

***Measured/Active Definitions are reserved for Windows/macOS systems because at this time we do not provide NGAV on Linux systems.**

COMMUNICATIONS

System Remediated Notification

At the conclusion of each handled incident, the EPP Team will send a summary report outlining what was observed, what actions were taken, and any required next steps. The notification will include the data elements shown in the following example.

Incident Details

System_Hostname:
JoePC

Username:
Administrator

System_IP_Address:
192.168.10.106

Detection_Scenario:
Known Malware - Ursnif

Detection_Severity:
HIGH

Detection_Details:
https://falcon.crowdstrike.com/activity/detections...

Date_of_Initial_Compromise:
20180611

Analysis_and_Remediation_Details:
The user fell victim to a phish which led to the installation of Ursnif malware.

Processes Stopped:
Markerscaler.exe

Quarantined Files:
C:\Users\Administrator\Downloads\Emails Models.docx
C:\Users\ Administrator\AppData\Local\Temp\67406.exe
C:\ProgramData\KdbNNb.exe
C:\Users\ Administrator\AppData\Local\Temp\ouxlfcbtocvpzpvhvgtsafmfds.txt
C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\exhphlda.miy
C:\Users\Administrator\AppData\local\Microsoft\Doetduo.wpq
C:\windows\SysWOW64\g3IhVX8KQNMnRx.exe

Removed Regkey's
HKCU\Software\Microsoft\Windows\Currentversion\Run
ychfmxl REG_SZ C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe "$windowsupdate =
\"C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe\"; & $windowsupdate"

Removed Scheduled Tasks related to the malware
125275F5-F470-4919-9A18-234F29DAB5C4
cmd.exe /C "start /MIN C:\windows\system32\cscript.exe //E:javascript "C:\Users\Administrator\AppData\Local\Microsoft\doetdu.wpq""

Recommended_Recovery_Tasks:
Reset Administrator password

Escalations

Escalations will be sent via email when the EPP Team requires action from you in order to remediate a system. Not having remote access to a system, needing approval to take additional remediation countermeasures, and recommendations to rebuild a system that has been irreparably damaged are examples of when an escalation will be sent via email.

The key difference between a System Remediated Notification and an Escalation is that Escalations require your action before the EPP Team can move forward with triage or remediation whereas System Remediated Notifications are those situations where the EPP Team has remediated a system(s) and is providing post-incident details of the actions taken to remediate the system(s).

Critical Escalations

When an escalation is required for a critical severity detection, the EPP Team will utilize the call roster provided by you in Appendix B to notify you.

Critical incidents are those incidents that involve:

- Destructive malware that was not blocked
- Interactive, hands on keyboard attacker
- Apparent theft of sensitive data (i.e. IP theft or PCI data)

During critical incident handling where remediation actions require approval or action needs to be taken by you during an incident, the EPP Team will attempt to call the phone numbers provided in Appendix B in order of priority. If there is no response from any of the contacts, the EPP Team will send a Critical Escalation email and continue monitoring but not proceed with any unapproved countermeasures.

In Appendix B, you will provide a contact list in order of priority when escalation is required.

METRICS

On a monthly basis, you will get an executive metrics dashboard that highlights the overall state of endpoint security in your environment, trended month over month. We will provide high level aggregate statistics that describe the performance of the solution covering two main areas.

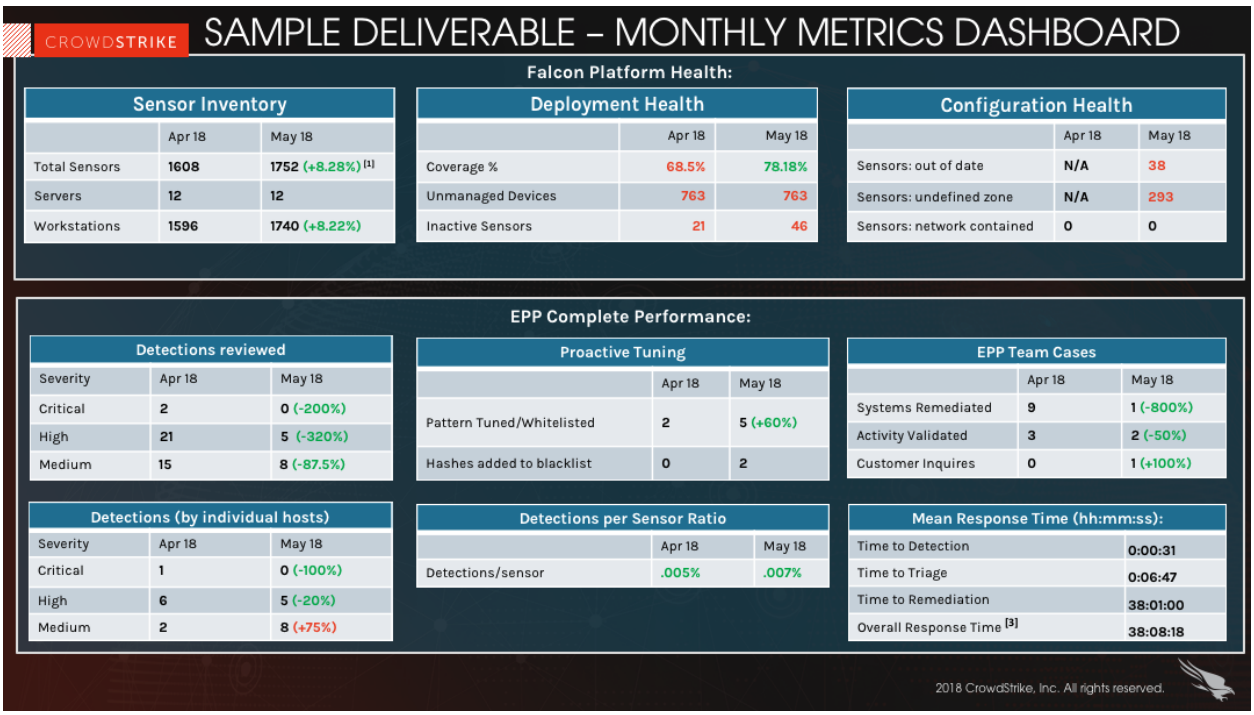
Falcon Platform Health:

- Information about the inventory of the sensor deployment
- Coverage information describing our understanding of the relative amount of the environment we believe to have deployed
- Information about the health of the sensors themselves, with respect to version management and prevention policy application

EPP Team Performance:

- Number of detections triaged by the team, also broken down by hosts
- Effort associated with improving the quality of detections in your environment through whitelisting and tuning of detections patterns
- Number and types of incidents and cases worked by the team
- Metrics about the speed of our response to detections we observe

Example monthly metrics dashboard:



CROWDSTRIKE SAMPLE DELIVERABLE – MONTHLY METRICS DASHBOARD

Falcon Platform Health:

Sensor Inventory	Apr 18	May 18
Total Sensors	1608	1752 (+8.28%) [1]
Servers	12	12
Workstations	1596	1740 (+8.22%)

Deployment Health	Apr 18	May 18
Coverage %	68.5%	78.18%
Unmanaged Devices	763	763
Inactive Sensors	21	46

Configuration Health	Apr 18	May 18
Sensors: out of date	N/A	38
Sensors: undefined zone	N/A	293
Sensors: network contained	0	0

EPP Complete Performance:

Detections reviewed		
Severity	Apr 18	May 18
Critical	2	0 (-200%)
High	21	5 (-320%)
Medium	15	8 (-87.5%)

Proactive Tuning	Apr 18	May 18
Pattern Tuned/Whitelisted	2	5 (+60%)
Hashes added to blacklist	0	2

EPP Team Cases	Apr 18	May 18
Systems Remediated	9	1 (-800%)
Activity Validated	3	2 (-50%)
Customer Inquires	0	1 (+100%)

Detections (by individual hosts)		
Severity	Apr 18	May 18
Critical	1	0 (-100%)
High	6	5 (-20%)
Medium	2	8 (+75%)

Detections per Sensor Ratio	Apr 18	May 18
Detections/sensor	.005%	.007%

Mean Response Time (hh:mm:ss):	
Time to Detection	0:00:31
Time to Triage	0:06:47
Time to Remediation	38:01:00
Overall Response Time [3]	38:08:18

SENSOR UPDATE POLICIES

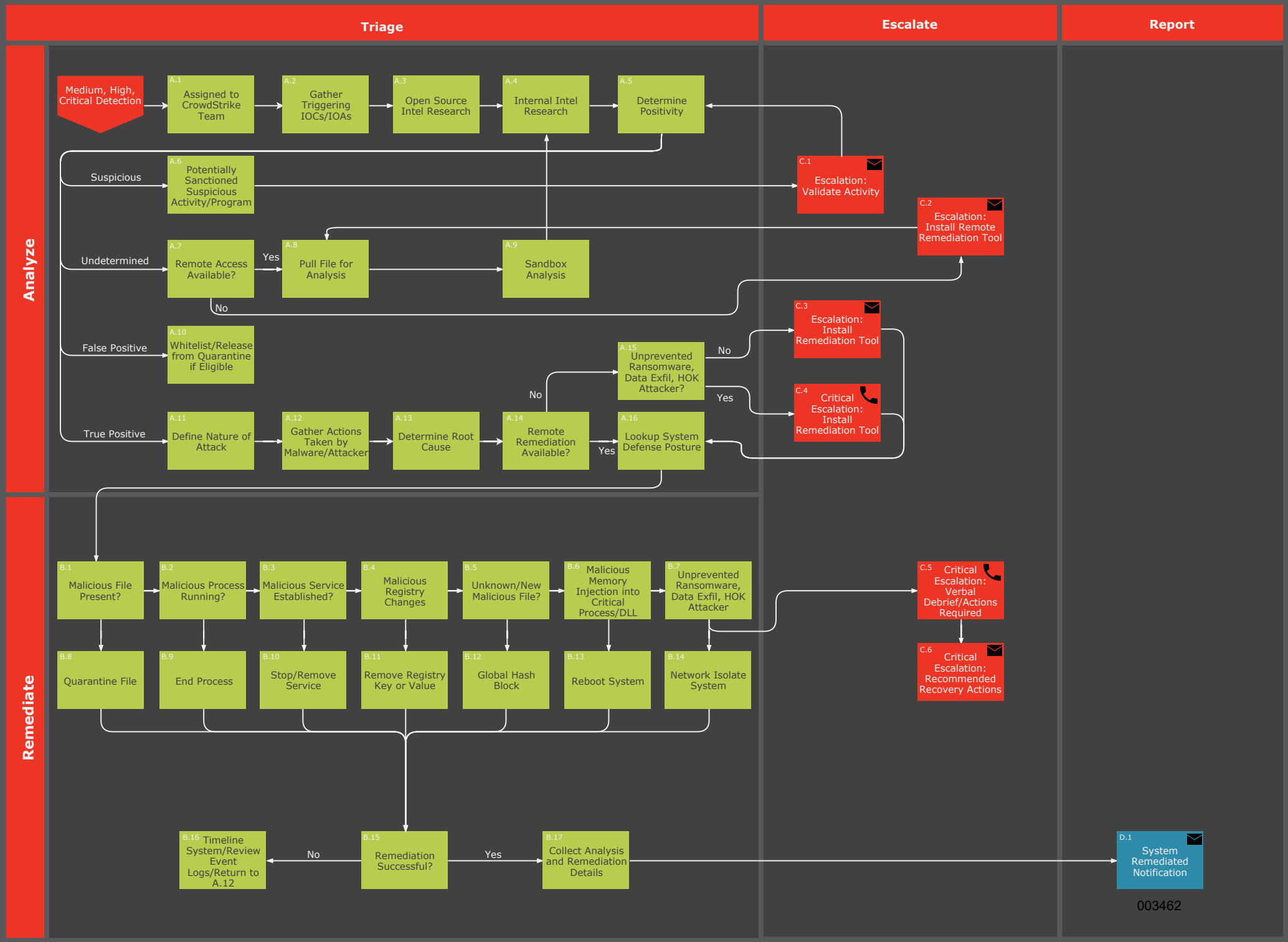
A Sensor Update Policy will be specified for each Asset Group in **Appendix B**.

This tells the EPP Team when you would like sensors upgraded as new versions are released and gives you the option and flexibility to roll out updates to different systems on a deferment schedule. The EPP Team will update sensors per asset group on your behalf according to the deferment set in Appendix B unless a problem is identified in which case the update may be placed on hold until resolved.

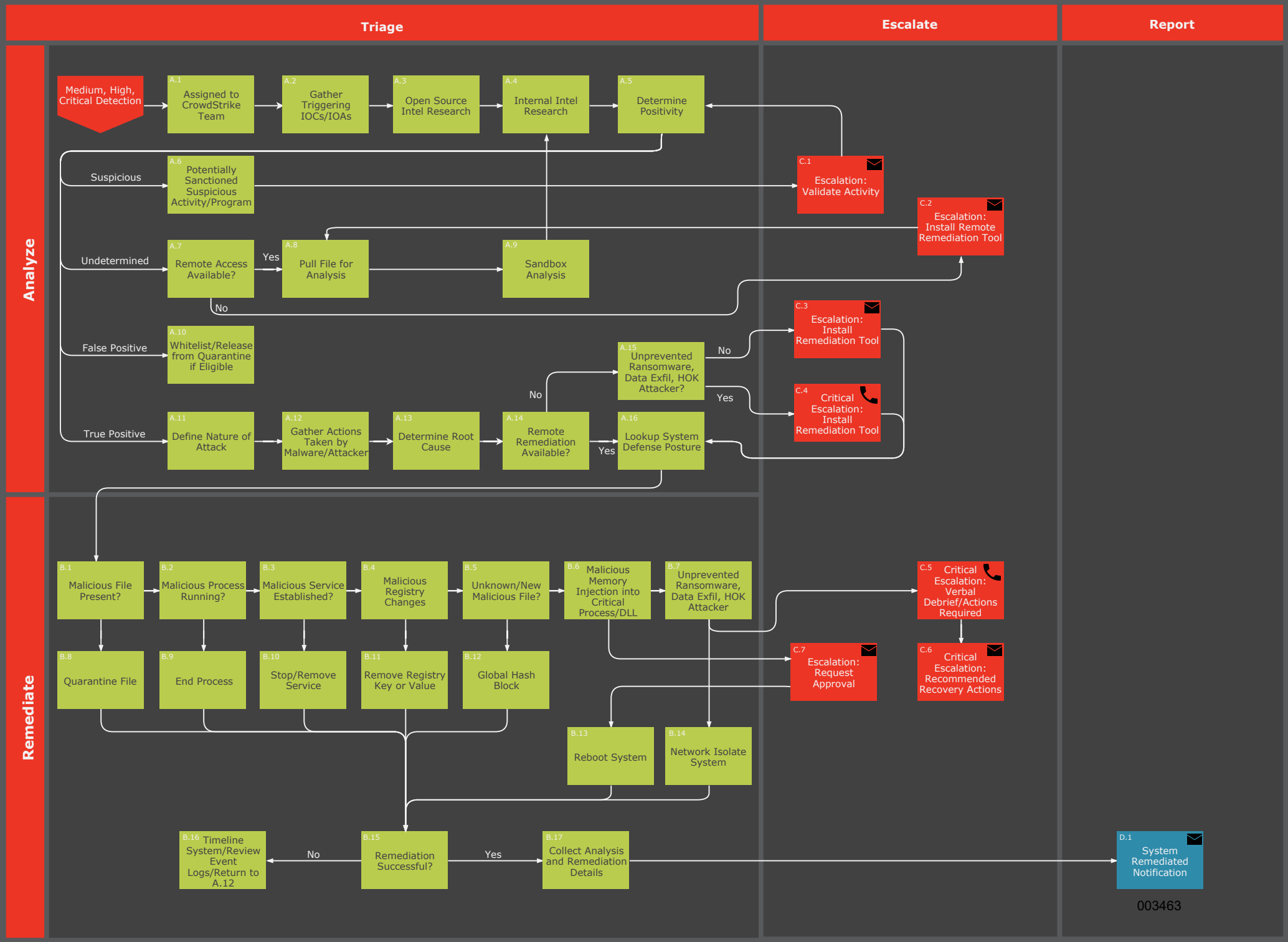
Updates can be set to Auto or on a weekly deferment of up to eight weeks.

EPP INCIDENT HANDLING WORKFLOWS

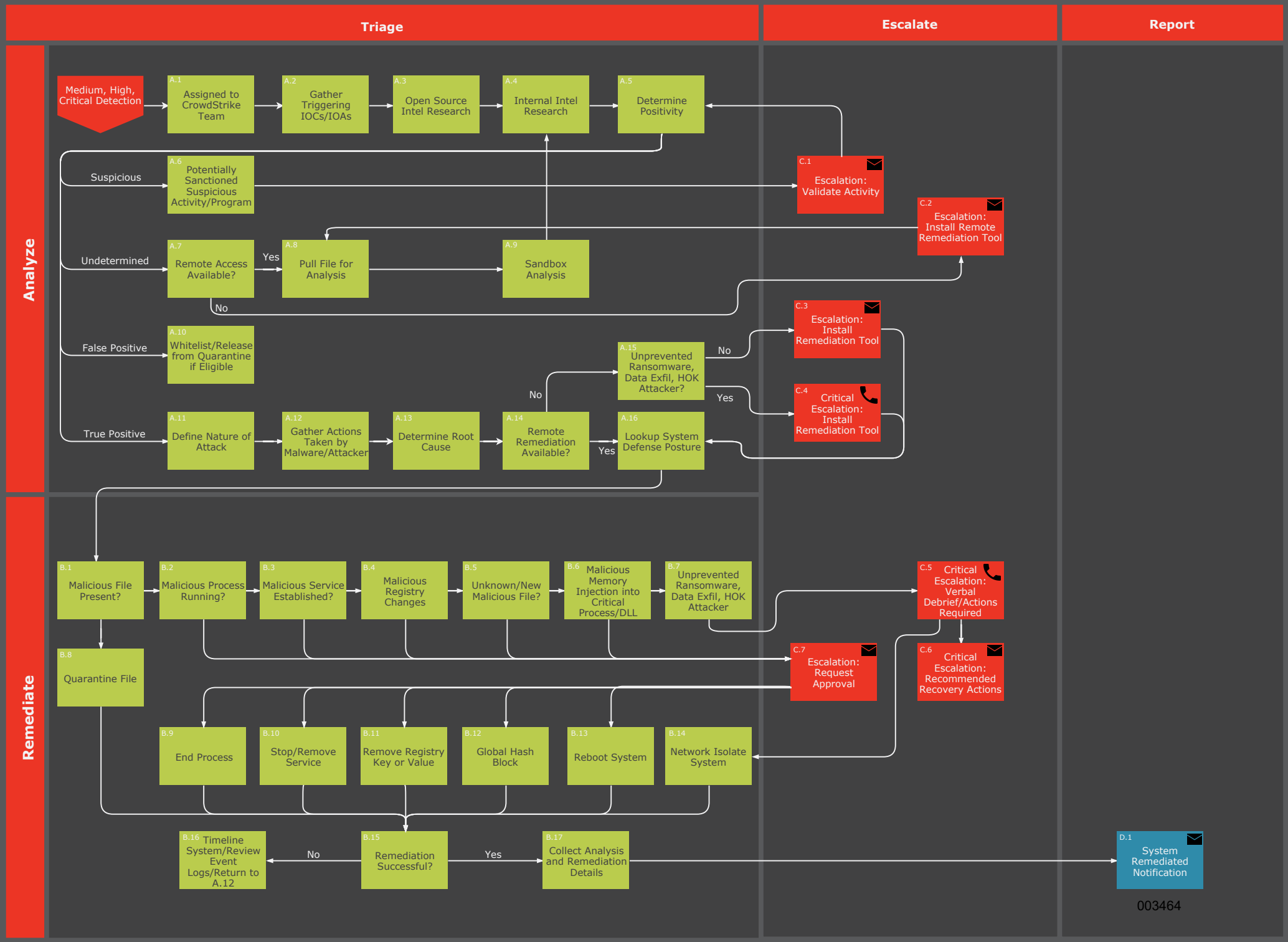
Playbook: Active Posture - EPP Complete



Playbook: Measured Posture - EPP Complete



Playbook: Cautious Posture - EPP Complete



COUNTERMEASURES EXPLAINED

Quarantine File

Suspected malicious files may be quarantined in place to prevent, cease, or remove a threat to a system or network. Quarantined files will typically be kept in an encrypted state on the host in the chance that the file needs to be restored.

Pull File for Analysis

On occasion, analysts may copy a suspected malicious file from a system for analysis to confirm if there is malicious behavior, code, or intent in the file. This will be done only when the malicious nature of a file is not certain and where hash blocking or quarantining the file without this analysis has the potential to disrupt.

Event Log Review

On occasion, analysts may conduct system forensics to include event log reviews, network analysis, file forensics, and registry reviews in order to confirm, contain, remediate, or eradicate malicious files or threat actors on a system.

End Process

On occasion, analysts may end a suspected malicious process in order to contain, remediate, or eradicate malware or a threat actor on a system.

Stop Service

On occasion, analysts may end a suspected malicious service in order to contain, remediate, or eradicate malware or a threat actor on a system.

Remove Registry Persistence

On occasion, analysts may remove a malicious registry object in order to contain, remediate, or eradicate malware or a threat actor on a system.

Global Process Hash Block

Processes identified as malicious may be placed into the process hash block list unique to your organization. This will block that processes hash across any system with the process hash blocking prevention enabled on the Falcon Platform Sensor.

Isolate System

On occasion, systems identified as dangerous to the network, to other systems, with potential C2 communications occurring, or with data exfiltration of potentially sensitive data may be placed in network isolation. Communications with the Falcon Platform will remain established but communication with other systems will not be allowed until taken out of isolation.

Restart System

On occasion, analysts may need to reboot a system to effectively remediate a compromise or infection.

OPERATIONS OVERVIEW

The EPP Team provides Falcon Platform management and managed threat response on a 24x7 basis. CrowdStrike will work with you to develop this document and its appendices as the mutually agreed upon method of operations. The EPP Operating Model will cover those endpoints on which the Falcon sensor has been installed and on boarded to one of the Playbook Security Postures ("Covered Endpoints"). In the event of a Falcon Platform detection, the EPP Team will act in accordance with the EPP Operating Model. The parties will mutually agree in the EPP Operating Model on the method for remediation, if any. The EPP Team will not perform remediation tasks that fall outside the scope of the countermeasures listed and as described within the EPP Operating Model.

The EPP Team does not perform: (i) forensic disk analysis, (ii) other advisory or consulting services, such as, but not limited to, systems configuration management, patch management, user awareness training, penetration testing, (iii) other strategic cyber security services, (iv) data recovery services for deleted, encrypted or otherwise lost data; or (iv) any services for any systems or endpoints other than Covered Endpoints.

Falcon Platform technical support addressing engineering issues with detections, platform performance, or platform function will be directed to CrowdStrike Support.

TRIAGE OVERVIEW

The EPP Team will triage Falcon detections according to the EPP Team Incident Handling Flowchart. Detections that are Medium, High, or Critical will be triaged for those systems that are Covered Endpoints.

Low detections are used by the EPP Team as additional information during an incident and will typically not be triaged on their own unless accompanied by a higher severity detection.

Duplicate detections or multiple detections on the same system that are identified by the EPP Team as part of one incident will often be grouped and triaged under one detection. This singular detection will reflect the assignment and status of EPP Team's work on that detection in the Falcon dashboard. The other related detections to the incident in the Falcon dashboard may be marked as ignored due to this grouping but are still being triaged, analyzed, and, where needed, responded to according to the Operating Model.

NEXT STEPS

Due From	Action Item	Due
You	Fill out Appendix B: Playbooks	Post onboarding call
You	Deploy ConnectWise globally	Until complete
You	Deploy Falcon globally	Until complete
CrowdStrike	Implement Asset Groups and Prevention Policies	After Receiving Completed Appendix B
CrowdStrike	Begin Managing Falcon Platform, Monitoring & Triaging Detections, and Remediating Systems	After Implementing Asset Groups and Prevention Policies

APPENDIX A: DATA ACCESS AND EVIDENCE HANDLING

Remote Remediation

Method

A lightweight agent, ConnectWise Control, is installed on each covered endpoint to facilitate remote remediation. ConnectWise Control is a secure cloud based remote access solution that provides remote remediation capabilities to the EPP Team.

Limited Access

The only employees of CrowdStrike that have access to the ConnectWise system are members of the EPP Team. EPP Team employees are residents of the USA, UK, or Australia. All members of the EPP Team are vetted through a background check prior to employment.

Access Controls

The EPP Team will access covered systems via TLS encryption and Multi-Factor Authentication (MFA). Each analyst account is authorized via password and second factor rotating key. ConnectWise allows for Role Based Access Control (RBAC) and the access performed by each account are tied to a specific analyst by name. Members of the EPP Team will only access systems for the purpose of incident triage or remediation. Any remediation actions done by an EPP Team analyst occur as a background task on the system account and are not visible to the end user.

Audit

Logs detailing the connections made by each user account as well as remote remediation commands sent by each user account are held active for a period of thirty (30) days by CrowdStrike. Any time EPP analysts take actions in a customer environment, a FLASH Notification will be sent outlining actions performed in coordination with a remediation event.

Monitoring and Segregation of Duties

In addition to access restriction controls and audit controls, every endpoint that has the ConnectWise agent on it also has the Falcon agent installed on it. Activities performed by the EPP Team will result in data that is observed by the Falcon agent. Activities associated with remediation tasks will be viewable by customers via the Falcon Insight module, and will also be hunted by OverWatch analysts, to create a high level of visibility into remediation tasks.

Evidence Handling

Throughout the course of an incident, further analysis may need to be conducted on select files from a covered system. This data is typically malware samples, event logs, or filesystem artifacts, and is rarely any user created binary content such as office documents. Any data collected for further analysis will be encrypted in transit and encrypted at rest. The EPP Team will utilize a secure file copy process to extract those select files from the system. Files of interest may include suspected malicious documents, suspected malicious binaries, files

potentially related to those malicious documents and binaries, and system event logs that may contain additional data points required to fully remediate a covered system.
Secure File Transfer Protocol (SFTP) is utilized to transfer files to a secure internal CrowdStrike Services forensics lab directory to which only the EPP Team has access. A write only SFTP account will be utilized to deliver files of interest selected by an analyst to the CrowdStrike forensics lab.
CrowdStrike does not retain any customer collected data for longer than necessary to conduct analysis and remediate an incident. Any collected evidence will not be shared outside of CrowdStrike.

CROWDSTRIKE

Falcon Endpoint Protection - COMPLETE

Operating Model

Table of Contents

OVERVIEW

CrowdStrike Falcon Endpoint Protection (EPP) Complete™ is a capability built on the CrowdStrike Falcon Platform. Customers gain market leading endpoint protection by combining Falcon Prevent (NGAV), Falcon Insight (EDR) and Falcon OverWatch (managed threat hunting). Additionally, the Falcon Endpoint Protection Team (EPP Team) manages and actively monitors the Falcon platform for you and remotely remediates incidents as needed. The CrowdStrike Falcon EPP Complete solution combines the effectiveness of the CrowdStrike Falcon platform with the efficiency of a dedicated team of CrowdStrike security professionals, executing focused incident handling playbooks.

We will work together to apply different playbook postures to the various asset groups you identify in your environment. We will configure sensor grouping and apply prevention postures to put your security strategy into action.

This document will establish the standard operating procedures and describe how the EPP Protection Team will work to manage the Falcon platform as well as respond to the various types of detections that the platform may generate.

PLAYBOOK SECURITY POSTURES

There are three Playbook Security Postures used by the EPP Team: Active Posture, Measured Posture, and Cautious Posture.

Each Playbook Security Posture determines how the Falcon Platform and the EPP Team handles a system in your environment.

Playbook Security Postures define two things:

1. The recommended configuration of the Falcon Platform prevention policies.
2. The countermeasures the EPP Team is pre-approved to use in remediating a system.

Playbook Posture Descriptions

Cautious:
Systems in Cautious Posture will have a lower risk of disruption by Falcon and the EPP Team but also a higher risk of compromise by malicious activity that does not have a high confidence detection. In this posture, remediation will take longer as countermeasures that are not pre-approved will need to be escalated to you for approval.

Highlights:

- Only non-disruptive remediation countermeasures are pre-approved.
- NGAV Prevention Policy set to prevent only High Severity detections.

Measured:
Systems in Measured Posture take a middle of the road approach allowing higher preventions from Falcon and all but inherently disruptive countermeasures as pre-approved. This allows for immediate prevention of potentially malicious activity that may not be prevented under Cautious Posture and allows for rapid remediation of compromised systems by the EPP Team. Lower confidence detections will not be prevented under this posture.

Highlights:

- Inherently disruptive Countermeasures not pre-approved (Reboot/Network Isolation).
- NGAV Prevention Policy set to prevent only Critical, High, and Medium severity detections.

Active:
Systems in Active Posture have the highest level of Falcon prevention and pre-approve the EPP Team to take any of the listed countermeasures required to remediate a system. Active Posture will mitigate the most amount of risk from malicious activity but may also cause an increase in false positive detections. These false positives will be identified and whitelisted on a case by case basis.

Highlights:

- All EPP Team Countermeasures pre-approved to remediate a compromised system.
- NGAV Prevention Policy set to prevent all levels of severity detections.

ASSET GROUPS

Asset Groups allow you to organize systems into groups and apply one of the three security postures to each group.[1]

This allows flexibility in how the EPP Team approaches different systems in your environment and how aggressive the Falcon Platform is configured to prevent potentially malicious activity.

Multiple Asset Groups are optional as you can choose to place all your assets in one group with one Playbook Posture applied or break down your assets in the Asset Group sheet in **Appendix B**. An example Asset Group assignment is shown below.

Criteria for assigning assets to a group will be defined in Appendix B.

Example Asset Group assignment:

Asset Group	Playbook Posture	Assignment Criteria
Workstations	Active Posture	OS Type
Servers	Measured Posture	OS Type
Critical Servers	Cautious Posture	CSV List
VIP Workstations	Measured Posture	CSV List

[1] Certain security postures may void warranty for asset groups

PLAYBOOK SECURITY POSTURES DETAILS

Windows - Falcon Platform Policy Configuration

Type	Category		Cautious Posture	Measured Posture	Active Posture
Sensor Capability	End User Notifications		Disabled	Disabled	Disabled
Sensor Visibility	Enhanced Visibility	Additional User Mode Data	Enabled	Enabled	Enabled
		Interpreter-Only	Enabled	Enabled	Enabled
		Engine (Full Visibility)	Disabled	Disabled	Enabled
Next-Gen Antivirus	Cloud Machine Learning	Cloud Anti-Malware Detection	Cautious	Aggressive	Aggressive
		Cloud Anti-Malware Prevention	Cautious	Moderate	Aggressive
		Adware/Pup Detection	Cautious	Moderate	Aggressive
		Adware/Pup Prevention	Cautious	Moderate	Aggressive
	Sensor Machine Learning	Sensor Anti-Malware Detection	Cautious	Aggressive	Aggressive
		Sensor Anti-Malware Prevention	Cautious	Moderate	Aggressive
	Quarantine	Quarantine & Security Center Registration	Enabled	Enabled	Enabled
Malware Protection	Execution Blocking	Custom Blacklisting	Disabled	Enabled	Enabled
		Prevent Suspicious Processes	Disabled	Enabled	Enabled
		Malicious PowerShell Scripts or Commands	Disabled	Enabled	Enabled
Behavior-Based Prevention	Exploit Mitigation Prevention	Force ASLR	Disabled	Disabled	Disabled
		Force DEP	Disabled	Disabled	Disabled
		Heap Spray Preallocation	Disabled	Enabled	Enabled
		NULL Page Allocation	Disabled	Disabled	Enabled

		SEH Overwrite Protection	Disabled	Disabled	Enabled
		Untrusted Font Loading	Disabled	Disabled	Enabled
		Remote Library Loading	Disabled	Disabled	Enabled
	Ransomware Prevention	Backup Deletion	Enabled	Enabled	Enabled
		Cryptowall	Enabled	Enabled	Enabled
		Ransomware File Extension	Enabled	Enabled	Enabled
		Locky	Enabled	Enabled	Enabled
		File System Access	Disabled	Disabled	Enabled
	Exploitation Behavior Prevention IOAs	Application Exploitation Activity	Disabled	Enabled	Enabled
		Chopper Webshell	Disabled	Enabled	Enabled
		Drive-by-Download	Disabled	Enabled	Enabled
		JavaScript Execution via Rundll32	Disabled	Enabled	Enabled
	Lateral Movement IOAs	Windows Logon Bypass Prevention	Enabled	Enabled	Enabled

Mac - Falcon Platform Prevention Policy Configuration

Type	Category		Cautious Posture	Measured Posture	Active Posture
Malware Protection	Machine Learning	File Attribution Detection	Cautious	Aggressive	Aggressive
		File Attribution Prevention	Cautious	Moderate	Aggressive
	Execution Blocking	Custom Hash Blacklisting	Disabled	Enabled	Enabled
		Prevent Suspicious Processes	Disabled	Enabled	Enabled
Behavior-Based Prevention	Unauthorized Remote Access IOAs	XPCOM Shell	Disabled	Enabled	Enabled
		Chopper Webshell	Disabled	Enabled	Enabled
		Empyre Backdoor	Disabled	Enabled	Enabled
	Credential Dumping IOAs	KcPassword Decoded	Disabled	Enabled	Enabled
		Hash Collector	Disabled	Enabled	Enabled

Countermeasures

During the course of incident handling, the EPP Team may need to take remediation actions. In accordance with this operating model, the table below describes at a high level what types of countermeasures are preapproved in each posture. When the EPP Team needs to implement countermeasures that are not preapproved, an escalation will be sent to you for approval.

Windows/macOS – EPP Complete Countermeasures

Analyst Countermeasure	Windows/macOS Cautious	Windows/macOS Measured	Windows/macOS Active
Quarantine File	x	x	x
Pull File for Analysis	x	x	x
Event Log Review	x	x	x
Global Process Hash Block		x	x
End Process		x	x
Stop Service		x	x
Disable Registry/PLIST Persistence		x	x
Isolate System		*	x
Restart System			x

*** System Isolation will still only be implemented for systems in Measured Posture in cases of data exfiltration or spreading ransomware.**

Linux – EPP Complete Countermeasures

Analyst Countermeasure	Linux Cautious	Linux Moderate*	Linux Agile*
Quarantine File	x	x	x
Pull File for Analysis	x	x	x
Event Log Review	x	x	x
Global Process Hash Block		x	x
End Process		x	x
Stop Service		x	x
Disable PLIST Persistence		x	x
Restart System			x

***Measured/Active Definitions are reserved for Windows/macOS systems because at this time we do not provide NGAV on Linux systems.**

COMMUNICATIONS

System Remediated Notification

At the conclusion of each handled incident, the EPP Team will send a summary report outlining what was observed, what actions were taken, and any required next steps. The notification will include the data elements shown in the following example table.

Incident Details

System_Hostname:
JoePC

Username:
Administrator

System_IP_Address:
192.168.10.106

Detection_Scenario:
Known Malware - Ursnif

Detection_Severity:
HIGH

Detection_Details:
https://falcon.crowdstrike.com/activity/detections...

Date_of_Initial_Compromise:
20180611

Analysis_and_Remediation_Details:
The user fell victim to a phish which led to the installation of Ursnif malware.

Processes Stopped:
Markerscaler.exe

Quarantined Files:
C:\Users\Administrator\Downloads\Emails Models.docx
C:\Users\ Administrator\AppData\Local\Temp\67406.exe
C:\ProgramData\KdbNNb.exe
C:\Users\ Administrator\AppData\Local\Temp\ouxlfcbtocvpzpvhvgtsafmfds.txt
C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\exhphlda.miy
C:\Users\Administrator\AppData\local\Microsoft\Doetduo.wpq
C:\windows\SysWOW64\g3IhVX8KQNMnRx.exe

Removed Regkey's
HKCU\Software\Microsoft\Windows\Currentversion\Run
ychfmxl REG_SZ C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe "$windowsupdate =
\"C:\Users\Administrator\AppData\Roaming\Microsoft\Doetduo\doetdu.exe\"; & $windowsupdate"

Removed Scheduled Tasks related to the malware
125275F5-F470-4919-9A18-234F29DAB5C4
cmd.exe /C "start /MIN C:\windows\system32\cscript.exe //E:javascript "C:\Users\Administrator\AppData\Local\Microsoft\doetdu.wpq""

Recommended_Recovery_Tasks:
Reset Administrator password

Escalations

Escalations will be sent via email when the EPP Team requires action from you in order to remediate a system. Not having remote access to a system, needing approval to take additional remediation countermeasures, and recommendations to rebuild a system that has been irreparably damaged are examples of when an escalation will be sent via email.

The key difference between a System Remediated Notification and an Escalation is that Escalations require your action before the EPP Team can move forward with triage or remediation whereas System Remediated Notifications are those situations where the EPP Team has remediated a system(s) and is providing post-incident details of the actions taken to remediate the system(s).

Critical Escalations

When an escalation is required for a critical severity detection, the EPP Team will utilize the call roster provided by you in Appendix B to notify you.

Critical incidents are those incidents that involve:

- Destructive malware that was not blocked
- Interactive, hands on keyboard attacker
- Apparent theft of sensitive data (i.e. IP theft or PCI data)

During critical incident handling where remediation actions require approval or action needs to be taken by you during an incident, the EPP Team will attempt to call the phone numbers provided in Appendix B in order of priority. If there is no response from any of the contacts, the EPP Team will send a Critical Escalation email and continue monitoring but not proceed with any unapproved countermeasures.

In Appendix B, you will provide a contact list in order of priority when escalation is required.

METRICS

On a monthly basis, you will get an executive metrics dashboard that highlights the overall state of endpoint security in your environment, trended month over month. We will provide high level aggregate statistics that describe the performance of the solution covering two main areas.

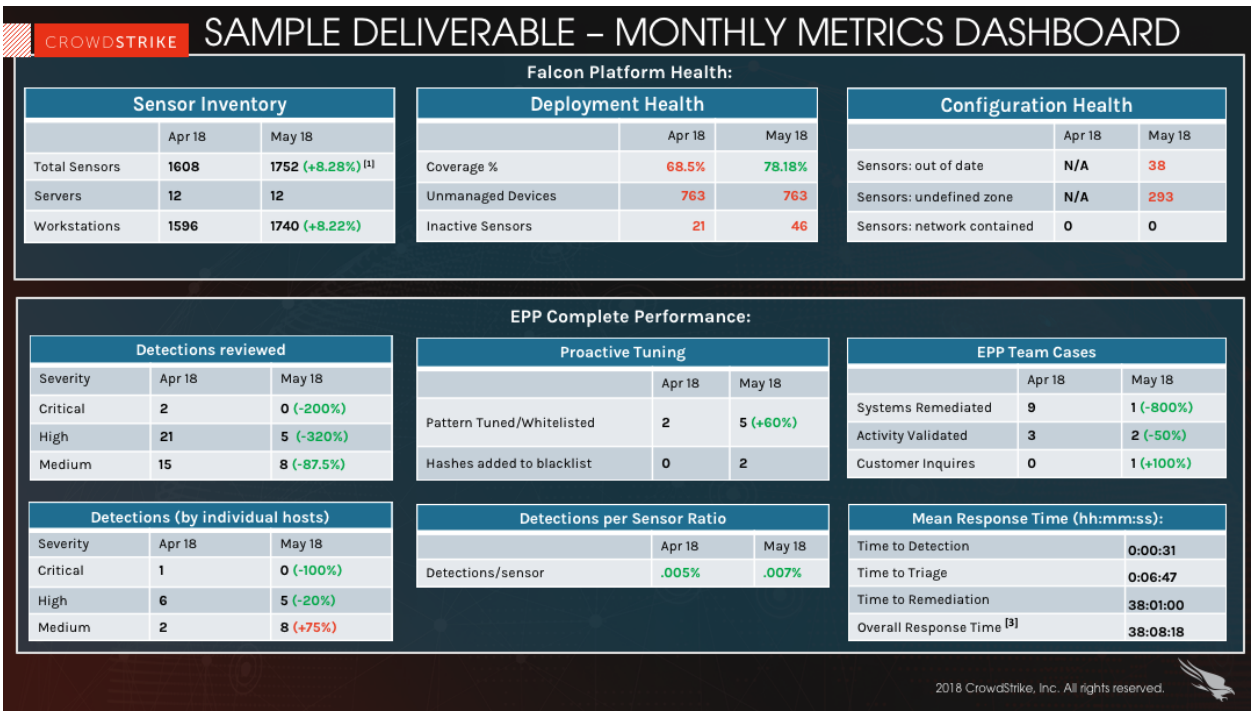
Falcon Platform Health:

- Information about the inventory of the sensor deployment
- Coverage information describing our understanding of the relative amount of the environment we believe to have deployed
- Information about the health of the sensors themselves, with respect to version management and prevention policy application

EPP Team Performance:

- Number of detections triaged by the team, also broken down by hosts
- Effort associated with improving the quality of detections in your environment through whitelisting and tuning of detections patterns
- Number and types of incidents and cases worked by the team
- Metrics about the speed of our response to detections we observe

Example monthly metrics dashboard:



CROWDSTRIKE SAMPLE DELIVERABLE – MONTHLY METRICS DASHBOARD

Falcon Platform Health:

Sensor Inventory	Apr 18	May 18
Total Sensors	1608	1752 (+8.28%) [1]
Servers	12	12
Workstations	1596	1740 (+8.22%)

Deployment Health	Apr 18	May 18
Coverage %	68.5%	78.18%
Unmanaged Devices	763	763
Inactive Sensors	21	46

Configuration Health	Apr 18	May 18
Sensors: out of date	N/A	38
Sensors: undefined zone	N/A	293
Sensors: network contained	0	0

EPP Complete Performance:

Detections reviewed		
Severity	Apr 18	May 18
Critical	2	0 (-200%)
High	21	5 (-320%)
Medium	15	8 (-87.5%)

Proactive Tuning	Apr 18	May 18
Pattern Tuned/Whitelisted	2	5 (+60%)
Hashes added to blacklist	0	2

EPP Team Cases	Apr 18	May 18
Systems Remediated	9	1 (-800%)
Activity Validated	3	2 (-50%)
Customer Inquires	0	1 (+100%)

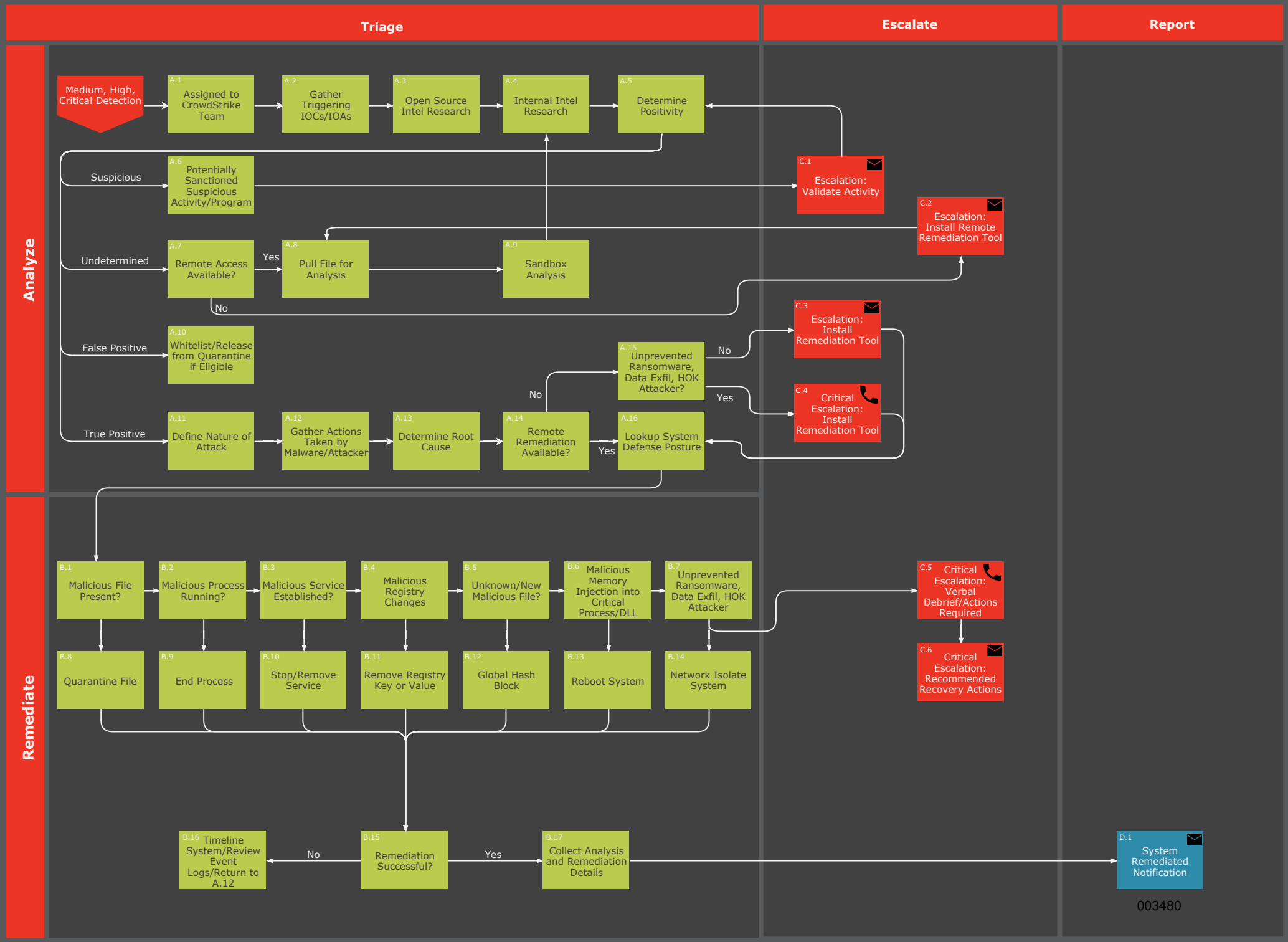
Detections (by individual hosts)		
Severity	Apr 18	May 18
Critical	1	0 (-100%)
High	6	5 (-20%)
Medium	2	8 (+75%)

Detections per Sensor Ratio	Apr 18	May 18
Detections/sensor	.005%	.007%

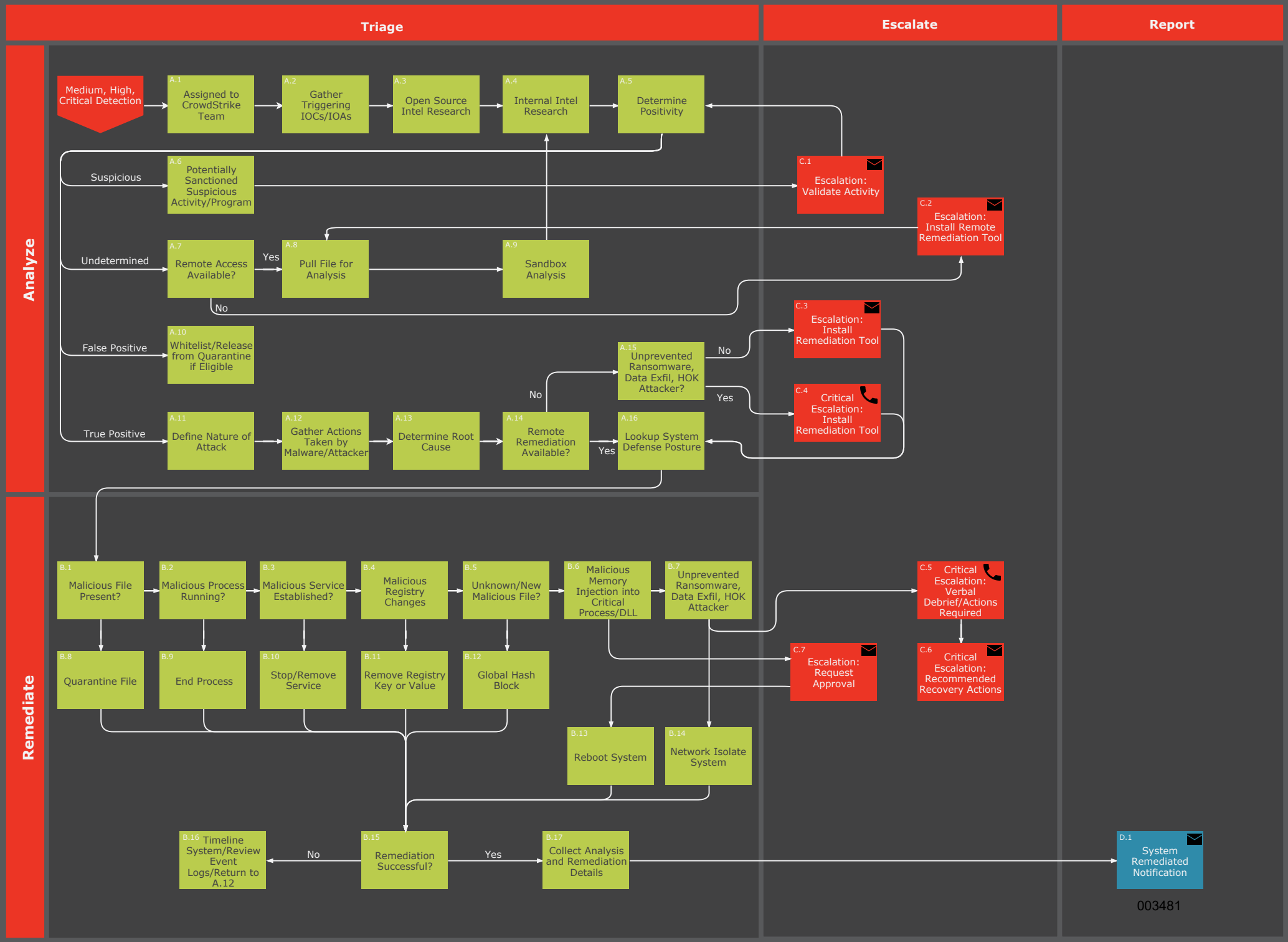
Mean Response Time (hh:mm:ss):	
Time to Detection	0:00:31
Time to Triage	0:06:47
Time to Remediation	38:01:00
Overall Response Time [3]	38:08:18

EPP INCIDENT HANDLING WORKFLOWS

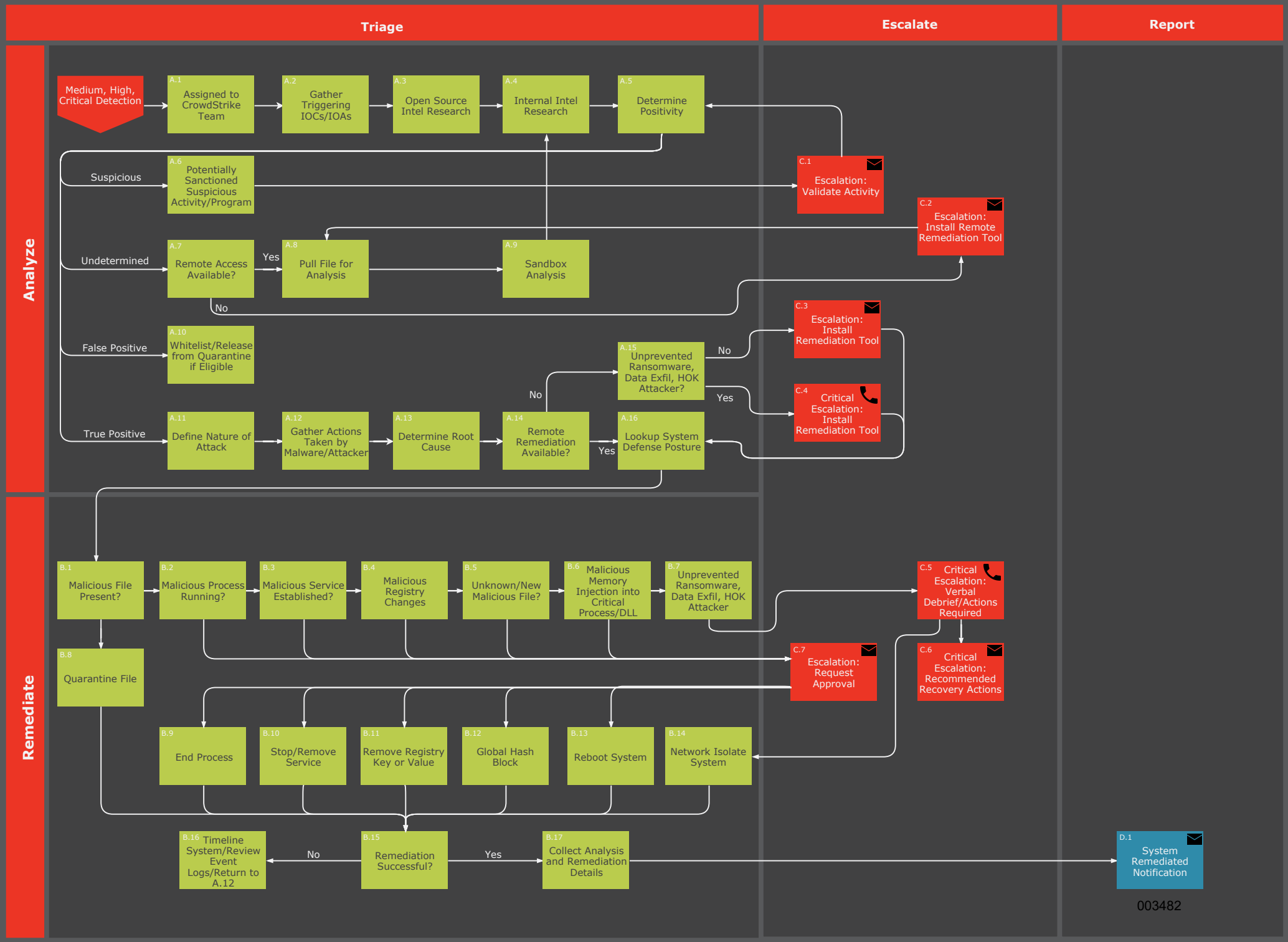
Playbook: Active Posture - EPP Complete



Playbook: Measured Posture - EPP Complete



Playbook: Cautious Posture - EPP Complete



FALCON PLATFORM CONFIGURATIONS EXPLAINED

End User Notifications

When enabled (Disabled by default), the Falcon Sensor will display pop-up notifications to the end user about actions taken to block or quarantine malicious files and activities. These messages can also be seen in the Windows Event Viewer under Applications and Services Logs.

Enhanced Visibility

Additional User Mode Data

Allows the sensor to gather additional data from the user-mode component by loading a library that hooks important system APIs. This data enables additional detections and augments online machine learning algorithms.

Interpreter Only

Provides visibility into malicious PowerShell interpreter usage.

Cloud Machine Learning

The Cloud Machine Learning category includes both Cloud Anti-malware and Adware & PUP. This cloud-based machine learning setting covers file attribute analysis and file analysis.
File attribute analysis aims to stop known malware that meets a specified certainty threshold. Instead of storing millions of known malware hashes on the client, CrowdStrike's Cloud AV provides real-time blocking against high-confidence known malware based on a combination of AV detection and file properties that are analyzed by the CrowdStrike cloud using machine learning. This protects against known malware without putting significant burden on the client. Each process is queried in real-time against our Cloud AV service and is prevented from executing if it matches high-confidence, known malware.

File analysis involves stopping malware that has been statically analyzed and flagged as malicious using CrowdStrike's machine learning techniques. These techniques allow for the analysis of files without the need to actually execute them. This, in turn, provides the capability to find new malware without the need for signatures and reliance on AV. What's more, because this happens in the cloud, there is no computational cost to the end user.

Adware and potentially unwanted programs (PUPs) are often considered just a nuisance, but they can be used to install malicious files.

Sensor Machine Learning

Provides machine learning-based on-sensor AV protection for malicious files, including offline protection.

Execution Blocking

Custom Blacklisting

Process hashes blocked in accordance with your organization's policy.

Prevent Suspicious Processes

Suspicious process identified by CrowdStrike based on dynamic Indicators-of-Attack (IOAs) to protect against malware, exploits and other threats.

Malicious PowerShell Scripts or Commands

A suspicious script or command identified by CrowdStrike was prevented from executing. Requires Interpreter-Only.

Exploit Mitigation Prevention

Force ASLR

Detected Address Space Layout Randomization (ASLR) bypass attempt.

Force DEP

Detected process that had Force Data Execution Prevention (Force DEP) applied attempting to execute non-executable memory.

Heap Spray Preallocation

Detected heap spray attempt.

Ransomware Prevention

Backup Deletion

Detected deletion of backups often indicative of ransomware activity.

Cryptowall

Detected process associated with Cryptowall.

File Encryption

Detected process that created a file with a known ransomware extension.

Locky

Detected process determined to be associated with Locky.

File System Access

Detected process associated with a high volume of file system operations typical of ransomware behavior.

Exploitation Behavior Prevention IOAs

Application Exploitation Activity

Detected creation of a process, such as a command prompt, from an exploited browser or browser flash plugin.

Chopper Webshell

Detected execution of a command shell indicative of the system hosting a Chopper web page.

Drive-by Download

Detected suspicious files written by a browser and attempted to execute.

JavaScript Execution Via Rundll32

Detected JavaScript executing from a command line via rundll32.exe.

Lateral Movement Prevention IOA

Windows Logon Bypass ("Sticky Keys")

Detected command line processes associated with Windows logon bypass.

COUNTERMEASURES EXPLAINED

Quarantine File

Suspected malicious files may be quarantined in place to prevent, cease, or remove a threat to a system or network. Quarantined files will typically be kept in an encrypted state on the host in the chance that the file needs to be restored.

Pull File for Analysis

On occasion, analysts may copy a suspected malicious file from a system for analysis to confirm if there is malicious behavior, code, or intent in the file. This will be done only when the malicious nature of a file is not certain and where hash blocking or quarantining the file without this analysis has the potential to disrupt.

Event Log Review

On occasion, analysts may conduct system forensics to include event log reviews, network analysis, file forensics, and registry reviews in order to confirm, contain, remediate, or eradicate malicious files or threat actors on a system.

End Process

On occasion, analysts may end a suspected malicious process in order to contain, remediate, or eradicate malware or a threat actor on a system.

Stop Service

On occasion, analysts may end a suspected malicious service in order to contain, remediate, or eradicate malware or a threat actor on a system.

Remove Registry Persistence

On occasion, analysts may remove a malicious registry object in order to contain, remediate, or eradicate malware or a threat actor on a system.

Global Process Hash Block

Processes identified as malicious may be placed into the process hash block list unique to your organization. This will block that processes hash across any system with the process hash blocking prevention enabled on the Falcon Platform Sensor.

Isolate System

On occasion, systems identified as dangerous to the network, to other systems, with potential C2 communications occurring, or with data exfiltration of potentially sensitive data may be placed in network isolation. Communications with the Falcon Platform will remain established but communication with other systems will not be allowed until taken out of isolation.

Restart System

On occasion, analysts may need to reboot a system to effectively remediate a compromise or infection.

OPERATIONS OVERVIEW

The EPP Team provides Falcon Platform management and managed threat response on a 24x7 basis. CrowdStrike will work with you to develop this document and its appendices as the mutually agreed upon method of operations. The EPP Operating Model will cover those endpoints on which the Falcon sensor has been installed and on boarded to one of the Playbook Security Postures ("Covered Endpoints"). In the event of a Falcon Platform detection, the EPP Team will act in accordance with the EPP Operating Model. The parties will mutually agree in the EPP Operating Model on the method for remediation, if any. The EPP Team will not perform remediation tasks that fall outside the scope of the countermeasures listed and as described within the EPP Operating Model.

The EPP Team does not perform: (i) forensic disk analysis, (ii) other advisory or consulting services, such as, but not limited to, systems configuration management, patch management, user awareness training, penetration testing, (iii) other strategic cyber security services, (iv) data recovery services for deleted, encrypted or otherwise lost data; or (iv) any services for any systems or endpoints other than Covered Endpoints.

Falcon Platform technical support addressing engineering issues with detections, platform performance, or platform function will be directed to CrowdStrike Support.

TRIAGE OVERVIEW

The EPP Team will triage Falcon detections according to the EPP Team Incident Handling Flowchart. Detections that are Medium, High, or Critical will be triaged for those systems that are Covered Endpoints.

Low detections are used by the EPP Team as additional information during an incident and will typically not be triaged on their own unless accompanied by a higher severity detection.

Duplicate detections or multiple detections on the same system that are identified by the EPP Team as part of one incident will often be grouped and triaged under one detection. This singular detection will reflect the assignment and status of EPP Team's work on that detection in the Falcon dashboard. The other related detections to the incident in the Falcon dashboard may be marked as ignored due to this grouping but are still being triaged, analyzed, and, where needed, responded to according to the Operating Model.

NEXT STEPS

Due From	Action Item	Due
You	Fill out Appendix B: Playbooks	Post onboarding call
You	Deploy ConnectWise globally	Until complete
You	Deploy Falcon globally	Until complete
CrowdStrike	Implement Asset Groups and Prevention Policies	After Receiving Completed Appendix B
CrowdStrike	Begin Managing Falcon Platform, Monitoring & Triaging Detections, and Remediating Systems	After Implementing Asset Groups and Prevention Policies

APPENDIX A: DATA ACCESS AND EVIDENCE HANDLING

Remote Remediation

Method

A lightweight agent, ConnectWise Control, is installed on each covered endpoint to facilitate remote remediation. ConnectWise Control is a secure cloud based remote access solution that provides remote remediation capabilities to the EPP Team.

Limited Access

The only employees of CrowdStrike that have access to the ConnectWise system are members of the EPP Team. EPP Team employees are residents of the USA, UK, or Australia. All members of the EPP Team are vetted through a background check prior to employment.

Access Controls

The EPP Team will access covered systems via TLS encryption and Multi-Factor Authentication (MFA). Each analyst account is authorized via password and second factor rotating key. ConnectWise allows for Role Based Access Control (RBAC) and the access performed by each account are tied to a specific analyst by name. Members of the EPP Team will only access systems for the purpose of incident triage or remediation. Any remediation actions done by an EPP Team analyst occur as a background task on the system account and are not visible to the end user.

Audit

Logs detailing the connections made by each user account as well as remote remediation commands sent by each user account are held active for a period of thirty (30) days by CrowdStrike. Any time EPP analysts take actions in a customer environment, a FLASH Notification will be sent outlining actions performed in coordination with a remediation event.

Monitoring and Segregation of Duties

In addition to access restriction controls and audit controls, every endpoint that has the ConnectWise agent on it also has the Falcon agent installed on it. Activities performed by the EPP Team will result in data that is observed by the Falcon agent. Activities associated with remediation tasks will be viewable by customers via the Falcon Insight module, and will also be hunted by OverWatch analysts, to create a high level of visibility into remediation tasks.

Evidence Handling

Throughout the course of an incident, further analysis may need to be conducted on select files from a covered system. This data is typically malware samples, event logs, or filesystem artifacts, and is rarely any user created binary content such as office documents. Any data collected for further analysis will be encrypted in transit and encrypted at rest. The EPP Team

will utilize a secure file copy process to extract those select files from the system. Files of interest may include suspected malicious documents, suspected malicious binaries, files potentially related to those malicious documents and binaries, and system event logs that may contain additional data points required to fully remediate a covered system.
Secure File Transfer Protocol (SFTP) is utilized to transfer files to a secure internal CrowdStrike Services forensics lab directory to which only the EPP Team has access. A write only SFTP account will be utilized to deliver files of interest selected by an analyst to the CrowdStrike forensics lab.
CrowdStrike does not retain any customer collected data for longer than necessary to conduct analysis and remediate an incident. Any collected evidence will not be shared outside of CrowdStrike.

CROWDSTRIKE

FALCON ENDPOINT PROTECTION **COMPLETE**™

A REVOLUTIONARY APPROACH TO ENDPOINT SECURITY

Complete endpoint security with unrivaled simplicity — guaranteed

FALCON ENDPOINT PROTECTION COMPLETE — TURNKEY ENDPOINT SECURITY THAT INCLUDES THE ONLY BREACH PREVENTION WARRANTY OF ITS KIND

A truly effective endpoint security solution requires a holistic approach. However, many organizations struggle to implement a comprehensive program because the time, cost and expertise needed are too high.

Falcon Endpoint Protection (EPP) Complete™ solves this problem by adding a team of security experts to handle every aspect of CrowdStrike® endpoint security technology for you. This powerful combination of people, processes and technology brings you to the highest level of endpoint security maturity without the burden of building it yourself. Falcon EPP Complete™ includes:

FALCON EPP COMPLETE™ SOLUTIONS

- **Falcon Prevent™** — next-gen antivirus with machine learning, exploit blocking, indicator of attack (IOA) behavioral analysis and more
- **Falcon Insight™** — endpoint detection and response (EDR)
- **Falcon Discover™** — IT hygiene and asset inventory
- **Falcon OverWatch™** — 24/7 managed threat hunting with managed detection and response (MDR)

FALCON EPP COMPLETE™ TEAM

- On-boarding
- Proactive configuration management
- Prevention health checks
- Maintenance and operations
- Incident handling playbook
- Incident triage and handling
- Hands-on remote remediation

TAKING ENDPOINT SECURITY TO THE NEXT LEVEL — THE BEST PROTECTION, 100 PERCENT MANAGED AND WORRY-FREE

Falcon EPP Complete provides the products and a seasoned team of experts to perform the tasks needed to handle all aspects of endpoint security, freeing you and your teams to focus on other important aspects of your business.

KEY BENEFITS

» Includes an exclusive warranty, for ultimate peace of mind

» Eliminates endpoint security burdens, providing effortless implementation, operations and incident remediation

» Provides remote remediation for timely, hassle-free incident resolution

» Offers the simplest and most effective endpoint security solution, accessible to all: Buy it and forget it

» Delivers immediate response and remediation anywhere

» Protects above and beyond traditional antivirus and other next-gen products

INCLUDES A BREACH PROTECTION WARRANTY OF UP TO $1 MILLION

In addition, Falcon EPP Complete is covered by a breach prevention warranty for the duration of the product subscription. The warranty provides up to $1 million of coverage to address any breach that occurs within the protected environment.

KEY PRODUCT CAPABILITIES

Falcon EPP Complete™ provides all the technologies and services required to instantly implement and continuously run a mature endpoint security program. It delivers the following benefits:

UNMATCHED NEXT-GEN EPP BENEFITS'

- **Guarantees protection:** Falcon EPP Complete comes with a breach protection warranty that covers the costs you would incur in responding to a breach, including legal services, client notification, identity theft and credit monitoring, forensics investigation and public relations.
- **Protects against all types of attacks:** Falcon EPP Complete™ protects your organization against commodity and zero-day malware, ransomware, exploits and advanced malware-free, fileless attacks — keeping you ahead of the rapidly changing tactics, techniques and procedures (TTPs) used by today's adversaries.
- **Combines the best prevention technologies:** For ultimate protection, Falcon EPP Complete™ combines technologies such as machine learning for malware protection, indicator of attack (IOA) behavioral blocking and exploit blocking.
- **Single, lightweight agent:** Falcon EPP Complete™ uniquely integrates powerful best-in-class prevention, detection and response, together with IT hygiene capabilities to provide continuous breach prevention in a single agent.

A FORCE MULTIPLIER: ALL THE HANDS-ON HELP AND EXPERTISE YOU NEED, WHEN YOU NEED IT

- **Gets you up and running and fully operational —** The Falcon EPP Team works with your organization to get you started and assists your team throughout the deployment process. During this interactive phase, CrowdStrike helps you understand the prevention capabilities of the Falcon platform and tailors these security postures to best fit your business and security needs.
- **Frees your IT and security teams from daily, time-consuming endpoint security tasks —** After initial implementation, the Falcon EPP Team administers the updates and maintenance of your solution, updating, monitoring and tuning Falcon to continually enhance your security posture. The team also reviews, triages, prioritizes and resolves alerts generated by the Falcon platform and Falcon OverWatch. The team identifies whether an alert is a false positive or a true incident and responds accordingly.
- **Reduces risk with immediate remote remediation of incidents —** When the Falcon EPP Team detects an incident, it can remotely remediate it. By ensuring that all incidents are handled immediately, Falcon EPP Complete™ dramatically reduces the risks of a serious breach. In addition, the Falcon EPP Team assists with guidance and expertise to help your teams with any security concerns they might have.

IMMEDIATE TIME-TO-VALUE

- **Easy deployment —** As part of the CrowdStrike platform, Falcon EPP Complete™ requires only the installation of a small 25 MB agent, without requiring management infrastructure or management consoles, making deployment easy and efficient.
- **Immediately operational —** Falcon EPP Complete™ can be deployed instantly for unrivaled time-to-value. As soon as it's installed, it hits the ground running, allowing the Falcon EPP Team to monitor and protect your organization without requiring additional components, reboots, query writing, staging or complex configuration.
- **Zero impact on performance —** Thanks to its cloud-native architecture, Falcon EPP Complete causes no additional impact on endpoints or the network.

ENDPOINT SECURITY AT ITS BEST

Falcon Endpoint Protection (EPP) Complete™ revolutionizes endpoint security by providing all of the components required for a mature endpoint security posture, from the initial setup and day-to-day operations to the prevention and detection of threats, all the way to full incident handling, including immediate remote remediation and recovery.

FALCON EPP COMPLETE: A UNIQUE SOLUTION

CrowdStrike Falcon EPP Complete™ is the only endpoint security solution with built-in proactive threat hunting and remote remediation, backed by a team of security experts that serves as your force multiplier, 24/7.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene, vulnerability management and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Learn more at **crowdstrike.com**

CROWDSTRIKE

FALCON ENDPOINT PROTECTION **COMPLETE**™

A REVOLUTIONARY APPROACH TO ENDPOINT SECURITY

Complete endpoint security with unrivaled simplicity — guaranteed

FALCON ENDPOINT PROTECTION COMPLETE — TURNKEY ENDPOINT SECURITY THAT INCLUDES THE ONLY BREACH PREVENTION WARRANTY OF ITS KIND

A truly effective endpoint security solution requires a holistic approach. However, many organizations struggle to implement a comprehensive program because the time, cost and expertise needed are too high.

Falcon Endpoint Protection (EPP) Complete™ solves this problem by adding a team of security experts to handle every aspect of CrowdStrike® endpoint security technology for you. This powerful combination of people, processes and technology brings you to the highest level of endpoint security maturity without the burden of building it yourself. Falcon EPP Complete™ includes:

FALCON EPP COMPLETE™ SOLUTIONS

- **Falcon Prevent™** — next-gen antivirus with machine learning, exploit blocking, indicator of attack (IOA) behavioral analysis and more
- **Falcon Insight™** — endpoint detection and response (EDR)
- **Falcon Discover™** — IT hygiene and asset inventory
- **Falcon OverWatch™** — 24/7 managed threat hunting with managed detection and response (MDR)

FALCON EPP COMPLETE™ TEAM

- On-boarding
- Proactive configuration management
- Prevention health checks
- Maintenance and operations
- Incident handling playbook
- Incident triage and handling
- Hands-on remote remediation

TAKING ENDPOINT SECURITY TO THE NEXT LEVEL — THE BEST PROTECTION, 100 PERCENT MANAGED AND WORRY-FREE

Falcon EPP Complete provides the products and a seasoned team of experts to perform the tasks needed to handle all aspects of endpoint security, freeing you and your teams to focus on other important aspects of your business.

KEY BENEFITS

» Includes an exclusive warranty, for ultimate peace of mind

» Eliminates endpoint security burdens, providing effortless implementation, operations and incident remediation

» Provides remote remediation for timely, hassle-free incident resolution

» Offers the simplest and most effective endpoint security solution, accessible to all: Buy it and forget it

» Delivers immediate response and remediation anywhere

» Protects above and beyond traditional antivirus and other next-gen products

INCLUDES A BREACH PROTECTION WARRANTY OF UP TO $1 MILLION

In addition, Falcon EPP Complete is covered by a breach prevention warranty for the duration of the product subscription. The warranty provides up to $1 million of coverage to address any breach that occurs within the protected environment.

KEY PRODUCT CAPABILITIES

Falcon EPP Complete™ provides all the technologies and services required to instantly implement and continuously run a mature endpoint security program. It delivers the following benefits:

UNMATCHED NEXT-GEN EPP BENEFITS'

- **Guarantees protection:** Falcon EPP Complete comes with a breach protection warranty that covers the costs you would incur in responding to a breach, including legal services, client notification, identity theft and credit monitoring, forensics investigation and public relations.
- **Protects against all types of attacks:** Falcon EPP Complete™ protects your organization against commodity and zero-day malware, ransomware, exploits and advanced malware-free, fileless attacks — keeping you ahead of the rapidly changing tactics, techniques and procedures (TTPs) used by today's adversaries.
- **Combines the best prevention technologies:** For ultimate protection, Falcon EPP Complete™ combines technologies such as machine learning for malware protection, indicator of attack (IOA) behavioral blocking and exploit blocking.
- **Single, lightweight agent:** Falcon EPP Complete™ uniquely integrates powerful best-in-class prevention, detection and response, together with IT hygiene capabilities to provide continuous breach prevention in a single agent.

A FORCE MULTIPLIER: ALL THE HANDS-ON HELP AND EXPERTISE YOU NEED, WHEN YOU NEED IT

- **Gets you up and running and fully operational —** The Falcon EPP Team works with your organization to get you started and assists your team throughout the deployment process. During this interactive phase, CrowdStrike helps you understand the prevention capabilities of the Falcon platform and tailors these security postures to best fit your business and security needs.
- **Frees your IT and security teams from daily, time-consuming endpoint security tasks —** After initial implementation, the Falcon EPP Team administers the updates and maintenance of your solution, updating, monitoring and tuning Falcon to continually enhance your security posture. The team also reviews, triages, prioritizes and resolves alerts generated by the Falcon platform and Falcon OverWatch. The team identifies whether an alert is a false positive or a true incident and responds accordingly.
- **Reduces risk with immediate remote remediation of incidents —** When the Falcon EPP Team detects an incident, it can remotely remediate it. By ensuring that all incidents are handled immediately, Falcon EPP Complete™ dramatically reduces the risks of a serious breach. In addition, the Falcon EPP Team assists with guidance and expertise to help your teams with any security concerns they might have.

IMMEDIATE TIME-TO-VALUE

- **Easy deployment —** As part of the CrowdStrike platform, Falcon EPP Complete™ requires only the installation of a small 25 MB agent, without requiring management infrastructure or management consoles, making deployment easy and efficient.
- **Immediately operational —** Falcon EPP Complete™ can be deployed instantly for unrivaled time-to-value. As soon as it's installed, it hits the ground running, allowing the Falcon EPP Team to monitor and protect your organization without requiring additional components, reboots, query writing, staging or complex configuration.
- **Zero impact on performance —** Thanks to its cloud-native architecture, Falcon EPP Complete causes no additional impact on endpoints or the network.

ENDPOINT SECURITY AT ITS BEST

Falcon Endpoint Protection (EPP) Complete™ revolutionizes endpoint security by providing all of the components required for a mature endpoint security posture, from the initial setup and day-to-day operations to the prevention and detection of threats, all the way to full incident handling, including immediate remote remediation and recovery.

FALCON EPP COMPLETE: A UNIQUE SOLUTION

CrowdStrike Falcon EPP Complete™ is the only endpoint security solution with built-in proactive threat hunting and remote remediation, backed by a team of security experts that serves as your force multiplier, 24/7.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene, vulnerability management and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Learn more at **crowdstrike.com**

The Forrester Wave™: Endpoint Security Suites, Q2 2018

The 15 Providers That Matter Most To Enterprises And How They Stack Up

by Chris Sherman and Salvatore Schiano
June 21, 2018

Why Read This Report

In our 21-criteria evaluation of endpoint security suite providers, we identified the 15 most significant ones — Bitdefender, Carbon Black, Check Point, Cisco, CrowdStrike, Cylance, ESET, Ivanti, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, Sophos, Symantec, and Trend Micro — and researched, analyzed, and scored them. This report shows how each provider measures up to help security professionals make the right choice.

Key Takeaways

Trend Micro, CrowdStrike, And Symantec Lead The Pack

Forrester's research uncovered a market in which Trend Micro, CrowdStrike, Symantec, Check Point, ESET, Sophos, and Bitdefender are Leaders; Carbon Black, McAfee, Kaspersky Lab, Cisco, Cylance, Microsoft, and Malwarebytes are Strong Performers; and Ivanti is a Challenger.

Security Pros Want An Effective Endpoint Security Suite From Vendors They Trust

Buyers want an endpoint security suite that is effective at stopping modern threats without adding to their security team's complexity. They also want to trust the vendor, both as a strategic partner and as a steward of their data.

Behavioral Analysis, Automation, And Real-World Performance Are Key Differentiators

As traditional approaches to endpoint security prove less effective, behavioral protection and suite automation have become key differentiators in today's market. Buyers also want to see real-world performance that backs up vendor claims.

The Forrester Wave™: Endpoint Security Suites, Q2 2018

The 15 Providers That Matter Most To Enterprises And How They Stack Up

by Chris Sherman and Salvatore Schiano
with Christopher McClean, Madeline Cyr, and Peggy Dostie

June 21, 2018

Table Of Contents

Related Research Documents

The Forrester Wave™: Endpoint Security Suites, Q4 2016

The State Of Endpoint Security, 2018

TechRadar™: Endpoint Security, Q1 2017

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Security Pros Are Demanding More-Effective Endpoint Security Suites

It's 2018, and employee endpoints continue to be the most targeted asset type in the enterprise.[1] Over the years, security teams have deployed a wide range of technologies to address threats to their corporate endpoints, and now many are opting for endpoint security suites with integrated prevention, detection, and automatic response. As vendors race to consolidate new methods of threat prevention with detection and response technologies, security teams have often found themselves unprotected due to gaps in coverage between products or they are otherwise unhappy with their choice of vendor and technology. Fundamental enterprise requirements are clear (see Figure 1):

- **Endpoint security suites must protect against modern threats.** It's no surprise that global enterprise security decision makers rate the evolving nature of IT threats as a top challenge.[2] As attackers continuously advance their methods to target gaps in traditional endpoint products, security pros look to their vendors to advance their protection capabilities. This includes the ability to block the global-scale attacks that are increasingly using techniques similar to those previously seen in targeted attacks (e.g., file-less malware and user exploitation), raising the bar substantially for security suite functional expectations.
- **They should decrease endpoint complexity.** IT environment complexity is another top challenge for global enterprise security decision makers; in fact, Forrester survey data shows that it's the most frequently cited challenging issue.[3] Complexity can come in many forms, but security teams are especially frustrated by deployment complexities that leave gaps in coverage, poorly laid out consoles that lead to challenging admin experiences, too many screens involved in day-to-day operations, and resources-draining performance issues like false positives and false negatives. Buyers want an endpoint security suite that consolidates capabilities and minimizes complexity when possible.
- **Vendors need to have strategies that inspire confidence.** More than ever, trust is critical in the endpoint security market. Buyers need to trust that their vendors will keep products up-to-date and effective against new attacks without significantly disrupting their business or exposing new vulnerabilities. Buyers also want to trust their endpoint security vendor to serve as a strategic partner in times of need, while inspiring confidence that the leadership team's vision will help prepare them for future challenges. Finally, buyers must trust that their vendors will be, without exception, good stewards of their corporate data.

FIGURE 1 A Modern Endpoint Security Suite Must Meet Three Fundamental Buyer Demands

Endpoint Security Suites Evaluation Overview

To assess the state of the endpoint security suites market and see how the vendors stack up against each other, Forrester evaluated the strengths and weaknesses of the top vendors. After examining past research, user need assessments, and vendor and expert interviews, we developed a comprehensive set of 21 criteria, which we grouped into three categories:

› **Current offering.** Each vendor's position on the vertical axis of the Forrester Wave™ graphic indicates the strength of its current offering. Key criteria for this evaluation include malware and exploit prevention, behavioral detection, and product performance, which Forrester validated using customer feedback and third-party test results.

› **Strategy.** Placement on the horizontal axis indicates the strength of the vendors' strategies. Here, we evaluated corporate vision and focus, security community involvement, and product road map.

› **Market presence.** Represented by the size of the markers on the graphic, our market presence scores reflect each vendor's enterprise customer base and licensing partner presence.

Evaluated Vendors And Inclusion Criteria

Forrester included 15 vendors in the assessment: Bitdefender, Carbon Black, Check Point, Cisco, CrowdStrike, Cylance, ESET, Ivanti, Kaspersky Lab, Malwarebytes, McAfee, Microsoft, Sophos, Symantec, and Trend Micro. Each of these vendors has (see Figure 2):

- **A security suite that can prevent, detect, and remediate endpoint threats.** We consider solutions that offer only one or two of these three capabilities to be point products, not suites.
- **A strong enterprise market presence.** We only included vendors with at least 100 enterprise customer accounts (1,000+ nodes deployed per enterprise) and at least one deployment with 100,000+ nodes.
- **A high degree of interest from enterprise buyers.** We only included vendors that garner substantial interest from enterprise security decision makers. For example, Forrester clients ask questions about each vendor by name during inquiries and other interactions.

FIGURE 2 Evaluated Vendors: Product Information And Inclusion Criteria

Vendor	Product evaluated	Version number
Bitdefender	GravityZone Endpoint Security	6.2
Carbon Black	Cb Defense	
Check Point	SandBlast Agent Complete Endpoint Protection	E80.81
Cisco	Advanced Malware Protection for Endpoints	6.0.9
CrowdStrike	CrowdStrike Falcon	4.1
Cylance	CylancePROTECT	2.0
ESET	ESET Endpoint Security	6.6
Ivanti	Ivanti Endpoint Security for Endpoint Manager	2017.3
Kaspersky Lab	Kaspersky Endpoint Security for Business (KESB)	11
Malwarebytes	Malwarebytes Endpoint Protection	1.1 (Windows); 1.5 (macOS)
McAfee	McAfee Endpoint Security	10.5.3
Microsoft	Windows Enterprise E5	E5
Sophos	Sophos Intercept X and Endpoint Protection	
Symantec	Symantec Endpoint Protection (SEP)	14.1
Trend Micro	Smart Protection Suite with Endpoint Sensor	

Vendor inclusion criteria
Integrated prevention, behavioral detection, and automatic remediation
More than 100 customers that have deployed vendor's endpoint software to 1,000+ nodes and at least one customer with more than 100,000 nodes
An established presence in the enterprise market with continuous interest from Forrester clients

Relevant Vendors Not Included In This Evaluation

There are many notable endpoint security vendors that receive interest from Forrester clients, but we didn't include them because they didn't meet one or more of our inclusion criteria. These vendors include Barkly, Comodo Cybersecurity, Cybereason, Endgame, FireEye, Palo Alto Networks, SentinelOne, and Webroot. Each of these vendors receive positive feedback from Forrester clients and are worthy of consideration, depending on your environment and requirements.

Vendor Profiles

This evaluation of the endpoint security suites market is intended to be a starting point only. We encourage clients to view detailed product evaluations and adapt criteria weightings to fit their individual needs through the Forrester Wave Excel-based vendor comparison tool (see Figure 3 and see Figure 4). Click the link at the beginning of this report on Forrester.com to download the tool.

FIGURE 3 Forrester Wave™: Endpoint Security Suites, Q2 2018

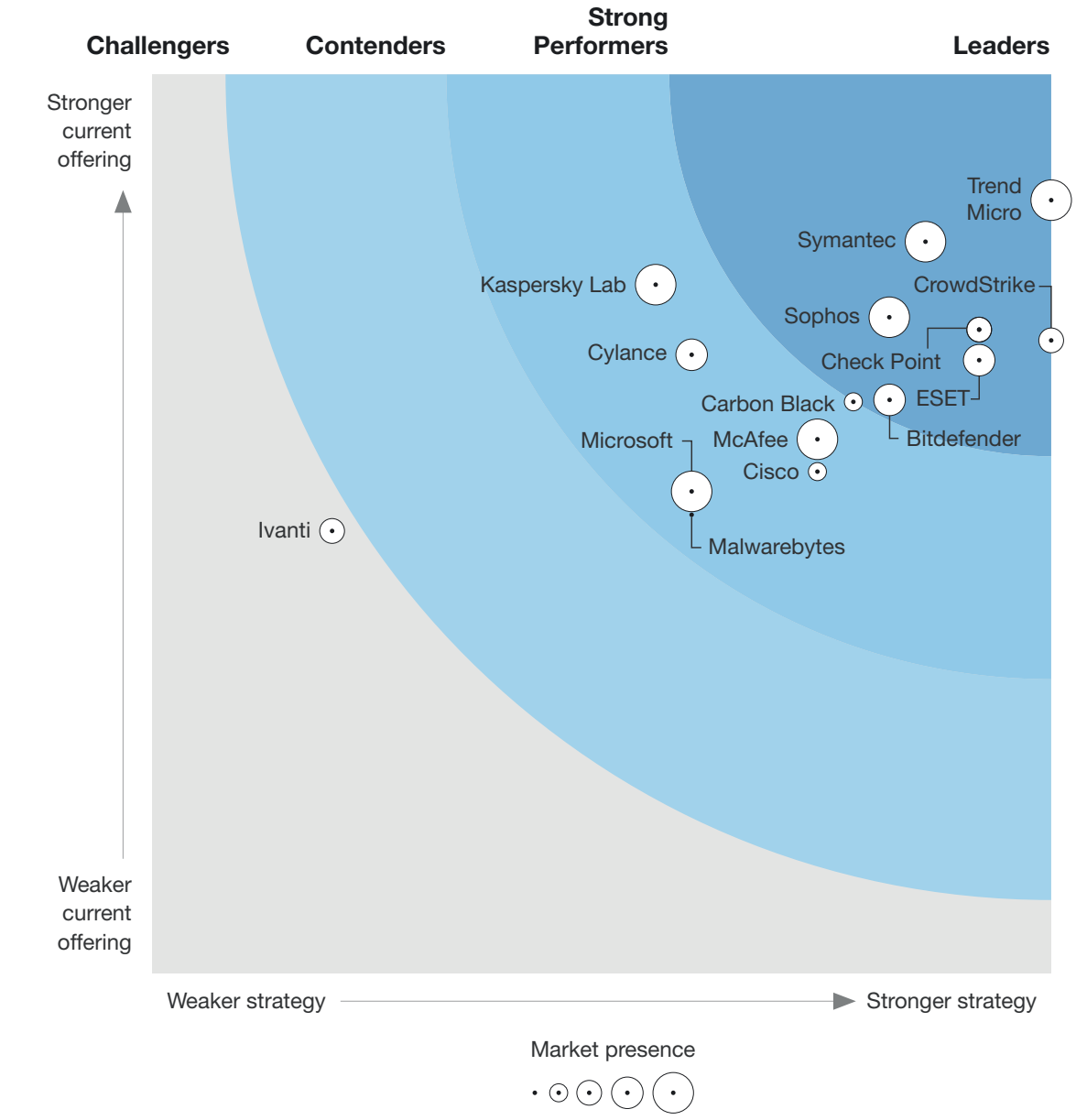


FIGURE 4 Forrester Wave™: Endpoint Security Suites Scorecard, Q2 2018

	Forrester's weighting	Bitdefender	Carbon Black	Check Point	Cisco	CrowdStrike	Cylance	ESET	Ivanti
Current Offering	50%	3.19	3.18	3.58	2.79	3.52	3.44	3.41	2.46
Threat prevention	20%	3.80	2.60	3.80	2.60	3.80	4.60	3.40	1.80
Threat detection	15%	2.00	5.00	3.00	4.00	5.00	3.00	4.00	1.00
Control	15%	2.20	3.40	3.00	1.00	1.80	3.00	2.20	5.00
Data security	8%	3.00	1.00	5.00	1.00	1.00	1.00	3.00	3.00
Mobile security	7%	3.00	1.00	5.00	3.00	3.00	1.00	3.00	3.00
Platform support	5%	5.00	3.00	3.00	5.00	5.00	3.00	5.00	5.00
Product performance	20%	4.00	3.50	2.60	3.90	4.00	4.10	4.00	1.00
External integrations	5%	3.00	5.00	5.00	1.00	5.00	5.00	3.00	1.00
Product support	5%	3.00	3.00	5.00	3.00	3.00	5.00	3.00	5.00
Strategy	50%	4.10	3.90	4.60	3.70	5.00	3.00	4.60	1.00
Product road map	20%	5.00	3.00	3.00	3.00	5.00	3.00	3.00	1.00
Security community involvement	35%	5.00	3.00	5.00	5.00	5.00	3.00	5.00	1.00
Corporate vision and focus	45%	3.00	5.00	5.00	3.00	5.00	3.00	5.00	1.00
Market Presence	0%	3.20	1.40	3.00	1.20	3.00	3.20	3.20	3.00
Enterprise customer base	90%	3.00	1.00	3.00	1.00	3.00	3.00	3.00	3.00
Licensing partner presence	10%	5.00	5.00	3.00	3.00	3.00	5.00	5.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

FIGURE 4 Forrester Wave™: Endpoint Security Suites Scorecard, Q2 2018 (Cont.)

	Forrester's weighting	Kaspersky Lab	Malwarebytes	McAfee	Microsoft	Sophos	Symantec	Trend Micro
Current Offering	50%	3.83	2.55	2.97	2.68	3.65	4.07	4.30
Threat prevention	20%	5.00	1.80	3.40	2.20	4.60	4.20	5.00
Threat detection	15%	4.00	4.00	2.00	3.00	2.00	4.00	3.00
Control	15%	3.40	3.40	5.00	2.20	2.20	4.20	4.20
Data security	8%	3.00	1.00	5.00	3.00	5.00	5.00	5.00
Mobile security	7%	3.00	1.00	1.00	3.00	5.00	5.00	5.00
Platform support	5%	5.00	1.00	3.00	1.00	5.00	5.00	5.00
Product performance	20%	4.10	2.40	1.60	2.30	4.50	3.00	4.10
External integrations	5%	3.00	3.00	5.00	5.00	1.00	5.00	5.00
Product support	5%	1.00	5.00	1.00	5.00	3.00	3.00	3.00
Strategy	50%	2.80	3.00	3.70	3.00	4.10	4.30	5.00
Product road map	20%	3.00	3.00	3.00	3.00	5.00	5.00	5.00
Security community involvement	35%	5.00	3.00	5.00	3.00	5.00	3.00	5.00
Corporate vision and focus	45%	1.00	3.00	3.00	3.00	3.00	5.00	5.00
Market Presence	0%	5.00	1.00	5.00	4.80	5.00	4.80	4.80
Enterprise customer base	90%	5.00	1.00	5.00	5.00	5.00	5.00	5.00
Licensing partner presence	10%	5.00	1.00	5.00	3.00	5.00	3.00	3.00

All scores are based on a scale of 0 (weak) to 5 (strong).

Leaders

- **Trend Micro continues to offer the most flexible and fully featured suite on the market.** Trend Micro maintains its position as a market leader with continuous evolution of its prevention and detection engines along with best-in-class suite capabilities. Customers give the product high marks for its malware and exploit prevention efficacy, with a low negative impact on endpoint user experience. Admins appreciate the product's high level of automation along with its flexibility and scalability to adapt to different operating environments. On the downside, Trend Micro's lack of integrated EDR (plans for this in 2H 2018) and only average customer scores for threat detection efficacy both present challenges for certain buyers. Regardless, Trend Micro is still an easy shortlist addition for most enterprise environments requiring a full endpoint security stack.
- **CrowdStrike has helped shape the mold for the modern endpoint security suite.** CrowdStrike started as an EDR vendor in 2012 but has evolved its offering into a highly automated suite, complete with threat prevention and multiple layers of automated detection and response. Compared to others in this study, CrowdStrike has superior exploit and behavioral detection capabilities, with customers reporting an above-average admin experience and easy deployments. Buyers appreciate the large ecosystem of partners and services, especially the aggressively priced OverWatch service, which provides proactive threat hunting for teams without advanced security expertise. However, some buyers will be turned off by CrowdStrike's high overall price and relatively little support for data security capabilities such as data encryption or data loss prevention. Nonetheless, Forrester expects CrowdStrike to continue showing up on the endpoint security suite shortlist among large and small enterprises for the foreseeable future.
- **Symantec's latest release shows its leadership is in touch with customer demands.** As the largest endpoint security company, Symantec often takes the brunt of the industry's backlash against ineffective antimalware. Customer feedback for Symantec had been low for years, and management turnover seemed to indicate Symantec was unwilling or unlikely to innovate in the near future. However, with the November 2016 release of SEP 14 and subsequent updates, the situation improved dramatically. Symantec delivered on its vision for a single-agent endpoint security product with consolidated signatureless malware prevention, best-of-breed detection capabilities, and automated response. These additions led to improved customer feedback on security efficacy and user experience. And while the company's customer feedback scores still reflect a nagging perception that Symantec is complex and ineffective, this will change as the company rebuilds trust and as more existing customers upgrade.
- **Check Point offers a fully featured, traditional suite with modern updates.** With its roots in network security, Check Point has expanded into other areas such as endpoint and mobile security over the years and today delivers an endpoint security suite that includes threat prevention, detection, data security, endpoint management, and mobile security. The product ships with multiple signatureless detection capabilities for malicious file/behavior, with tight integration to share policy and threat intel between the company's endpoint, network, and cloud offerings.

Unfortunately, customers reported a higher impact to endpoint user experience compared to other products in this report. Overall, for customers looking for a solid combination of new technology and traditional suite capabilities in a single console, Check Point should easily make the shortlist.

- **ESET combines threat prevention and detection with a focus on user experience.** ESET's endpoint security suite brings together multiple scanning and behavioral detection engines to deliver strong malware and exploit prevention, while preserving the endpoint user experience. The company has been focused on maintaining a low false positive rate and a light touch on the endpoint since its first enterprise product, and customers continually rate them above average in endpoint user experience. In addition to the core threat prevention and detection tools, the product also includes a handful of ancillary endpoint security tools such as native encryption management and mobile antimalware. On the downside, ESET's detection and response functionality will likely be a deterrent for teams looking for advanced response workflows. The relative basic vulnerability management capabilities may also be an issue for some buyers. Overall, ESET is best for enterprises looking for a full suite that requires low expertise for operation.
- **Sophos shows that machine learning can keep traditional suite vendors relevant.** Sophos offers a broad, tightly integrated portfolio of endpoint security tools that target smaller enterprises. When customers began to demand better protection against fileless malware and advanced attacks from their traditional endpoint security suite vendors in 2017, Sophos acquired Invincea and subsequently integrated its machine learning (ML) models into the Sophos Intercept X product, which provides exploit prevention, anti-ransomware features, and root cause analysis for incident forensics. Today, Sophos offers most of the major suite capabilities important to enterprise buyers, all managed through a cloud platform, with the exception of patch management. Customer satisfaction is very high for both the admin experience and low impact to endpoint performance. One drawback is that it currently lacks an EDR capability in the market (planned in an upcoming release). For enterprise buyers looking for a full prevention-oriented suite, Sophos is an easy shortlist addition.
- **Bitdefender offers threat prevention across a wide range of endpoint platforms.** Enterprise interest in Bitdefender has increased over the past two years as the company has expanded its reach through licensing partnerships and has focused on delivering an integrated, easy-to-use threat prevention and detection solution. One of Bitdefender's major differentiators is the reach of its sensor network. Since Bitdefender has specialized in licensing its core engine to vendors outside of the traditional endpoint security space (everything from network appliances to IoT devices), its threat research covers a broad range of attack vectors. Customers report above-average prevention capabilities and a low detriment to endpoint user experience. However, for teams looking for more advanced threat hunting and detection capabilities, Bitdefender lacks many of the analysis and response capabilities offered by market leaders. Bitdefender is well-suited for large and small environments with less need for sophisticated detection.

Strong Performers

- **Cb Defense moves Carbon Black into the broader market.** Carbon Black's Cb Defense (formerly Confer) is a cloud-based single-agent suite that provides integrated threat prevention and detection. While Cb Defense delivers above-average detection efficacy (determined through customer feedback), strong behavioral analysis, and superior endpoint visibility, it lacks some features found in established products such as patch management, data loss protection, and mobile security. Because of the sophisticated customizable rules available for detection configuration, admins also report a high level of expertise required to run the product. Overall, Cb Defense is best for security teams looking to build or augment their endpoint behavioral protection, especially those with the expertise to take advantage of the product's more advanced features.
- **McAfee is working to regain customer confidence with technical improvements.** McAfee's endpoint security products have been plagued with deployment challenges and low efficacy, but the latest version of Enterprise Security (ENS) seems to have solved these issues with a re-architected console and machine learning capabilities integrated into the local prevention engine. McAfee is hoping these technical improvements will help convince the company's large customer base to migrate to the latest version instead of opting for a replacement product. But there will be challenges; McAfee still gets low scores for admin experience and efficacy, and its products still don't support mobile devices. McAfee will likely improve customer perceptions and increase adoption of its new versions if it executes on its vision to simplify security through third-party integrations and automation.
- **Kaspersky Lab is struggling to win back customer trust despite having strong tech.** Kaspersky Lab has offered one of the most technically capable enterprise endpoint security products for years. This technical dominance continues in 2018, with the company getting above-average customer feedback for the product's malware and exploit prevention technologies, along with improvements to the suite's admin capabilities and UI. Unfortunately, this functional breadth and depth is overshadowed by a high level of distrust among US and EU buyers due to multiple government bans of Kaspersky software and perceived corporate instability. While buyers in other geographies are likely to continue to use Kaspersky products due to their technical merit, it remains to be seen whether Kaspersky's recent corporate initiatives (e.g., Global Transparency Initiative and movement of key business operations to Switzerland) will be successful at regaining customer trust in those markets where bans are in place.
- **Cisco's endpoint security offering delivers the modern essentials.** Cisco's AMP for Endpoints delivers malware and exploit prevention, behavioral detection, and automated response in a single agent on a broad number of endpoint types, with few ancillary capabilities outside of these fundamentals. Cisco relies heavily on its own threat research as well as customer-derived data from the Cisco Threat Grid and Threat Intelligence Cloud; data collected can be easily consumed by other Cisco security services/offerings (such as its managed detection and response service). While some of the product's detection capabilities are quite advanced, admins rate the product

as easy to use with very positive feedback on admin experience and user experience preservation compared to the overall average. For existing customers of Cisco services or buyers with few suite requirements, AMP for Endpoints may be ideal.

- **Cylance offers superior threat prevention but falls short on detection.** When Cylance released its first product in 2012, the company proved to enterprises that prevention isn't dead; it had simply evolved to a new level using machine learning. Cylance was the first to show that machine learning technology, when trained correctly, can accurately classify files without constant model updating or signatures. Today, CylancePROTECT still stands as one of the best prevention-focused tools on the market, but customers reported that their detection efficacy is a clear weak point. Suite capabilities such as mobile security and data security are also lacking today. Forrester sees most large enterprises layering Cylance on top of detection-focused products today, but as Cylance executes on its vision to build out more suite capabilities and ML-based detection (released after the evaluation period but before publication), Forrester expects this to change.
- **Microsoft offers a serious alternative to third-party endpoint security suites.** Microsoft has slowly ramped up its focus on endpoint security over the past five years, giving Windows 10 improved efficacy against unknown malware and exploits, stronger application security, and innovative data security measures. The company also offers endpoint detection and basic response capabilities with its Advanced Threat Protection (ATP) offering, but it requires additional partner tools to cover non-Windows endpoints. Buyers complain that the various components in a full Microsoft Windows 10 security stack require multiple consoles to manage policies. However, companies that have standardized on Windows 10 and have the latest hardware and security features enabled would be hard pressed to find another vendor in this study with better exploit protection. Buyers with a more fragmented device environment or more advanced detection requirements are likely to get more value augmenting Microsoft's security features for prevention with a detection-focused suite.
- **Malwarebytes aims to move beyond its supporting role in your security stack.** Malwarebytes has only recently shown interest in the enterprise security suite space, while the company's free remediation tools have been a staple for security and IT ops admins for over a decade. With the latest version of Malwarebytes Endpoint Protection, enterprise buyers get malware and exploit prevention, detection, and best-of-breed remediation in one product. Customer feedback is very high for the product's behavioral detection and remediation capabilities, but this is countered by lower-than-average malware prevention scores as determined by Forrester analysis and customers of the product. Likely for this reason, enterprises still primarily use Malwarebytes in a supporting role side by side with other prevention-oriented security point products and suites, but this will change as the company builds more enterprise-grade functionality (e.g., more third-party integrations, modern suite functions covering data security and vulnerability management, more robust malware execution prevention, etc.) into the product. Overall, Malwarebytes is perfect for enterprises looking for a basic suite replacement or as an additional layer of protection where behavioral detection/remediation is lacking.

Challengers

› **Ivanti bridges the divide between IT ops and security.** Ivanti formed in 2017 when LANDESK and HEAT Software merged. This background gives the company a deep bench of application control, patch management, and endpoint management product capabilities, leading to a high amount of credibility with IT ops professionals compared to most endpoint security suite vendors. However, rather than continue developing its own threat prevention and detection solution, the company offers customers a range of threat prevention and detection technologies through OEM partnerships. This means that the company's security offerings aren't better or worse than many others in this study, although large enterprise security teams looking for strong app control with a low requirement for advanced threat detection or prevention capabilities beyond AV should consider Ivanti.

Supplemental Material

Online Resource

The online version of Figure 3 is an Excel-based vendor comparison tool that provides detailed product evaluations and customizable rankings. Click the link at the beginning of this report on Forrester.com to download the tool.

Data Sources Used In This Forrester Wave

Forrester used a combination of three data sources to assess the strengths and weaknesses of each solution. We evaluated the vendors participating in this Forrester Wave, in part, using materials that they provided to us by March 20, 2018.

- **Vendor surveys.** Forrester surveyed vendors on their capabilities as they relate to the evaluation criteria. Once we analyzed the completed vendor surveys, we conducted vendor calls where necessary to gather details of vendor qualifications.
- **Product demos.** We asked vendors to conduct demonstrations of their products' functionality. We used findings from these product demos to validate details of each vendor's product capabilities.
- **Customer reference calls.** To validate product and vendor qualifications, Forrester also conducted reference calls or surveys with at least three of each vendor's current customers.

The Forrester Wave Methodology

We conduct primary research to develop a list of vendors that meet our criteria for evaluation in this market. From that initial pool of vendors, we narrow our final list. We choose these vendors based on: 1) product fit; 2) customer success; and 3) Forrester client demand. We eliminate vendors that have limited customer references and products that don't fit the scope of our evaluation. Vendors marked as incomplete participants met our defined inclusion criteria but declined to participate or contributed only partially to the evaluation.

After examining past research, user need assessments, and vendor and expert interviews, we develop the initial evaluation criteria. To evaluate the vendors and their products against our set of criteria, we gather details of product qualifications through a combination of lab evaluations, questionnaires, demos, and/or discussions with client references. We send evaluations to the vendors for their review, and we adjust the evaluations to provide the most accurate view of vendor offerings and strategies.

We set default weightings to reflect our analysis of the needs of large user companies — and/or other scenarios as outlined in the Forrester Wave evaluation — and then score the vendors based on a clearly defined scale. We intend these default weightings to serve only as a starting point and encourage readers to adapt the weightings to fit their individual needs through the Excel-based tool. The final scores generate the graphical depiction of the market based on current offering, strategy, and

market presence. Forrester intends to update vendor evaluations regularly as product capabilities and vendor strategies evolve. For more information on the methodology that every Forrester Wave follows, please visit The Forrester Wave™ Methodology Guide on our website.

Integrity Policy

We conduct all our research, including Forrester Wave evaluations, in accordance with the Integrity Policy posted on our website.

Survey Methodology

The Forrester Analytics Global Business Technographics® Security Survey, 2017 was fielded between May and June of 2017. This online survey included 3,752 respondents in Australia, Brazil, Canada, China, France, Germany, India, New Zealand, the UK, and the US from companies with two or more employees.

Forrester Analytics' Business Technographics ensures that the final survey population contains only those with significant involvement in the planning, funding, and purchasing of business and technology products and services. Research Now fielded this survey on behalf of Forrester. Survey respondent incentives include points redeemable for gift certificates.

Please note that the brand questions included in this survey should not be used to measure market share. The purpose of Forrester Analytics' Business Technographics brand questions is to show usage of a brand by a specific target audience at one point in time.

Endnotes

[1] See the Forrester report "The State Of Endpoint Security, 2018."

[2] Source: Forrester Analytics Global Business Technographics Security Survey, 2017.

[3] Source: Forrester Analytics Global Business Technographics Security Survey, 2017.

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.

Critical Capabilities for Endpoint Protection Platforms

Published: 30 April 2018 **ID:** G00334896

Analyst(s): Eric Ouellet, Ian McShane

Endpoint protection is evolving to address security architecture tasks such as hardening, investigation, incident detection and incident response. Security and risk management leaders should evaluate EPP vendors' ability to keep up with modern endpoint threats and their deployment requirements.

Key Findings

- Advanced prevention capabilities such as machine learning, software behavior analytics and exploit prevention are no longer only available from newer EPP vendors; rather, they have become part of the core set of prevention solutions offered by nearly all vendors in this market.
- Many Type B organizations want to incorporate advanced EDR capabilities as a means of actively detecting and responding to threats; however, EDR solutions remain challenging to deploy and operate for most.
- Most Type B and Type C organizations eventually elect to use EDR as a forensics-focused solution if they operate it themselves, or they opt to engage managed services to supplement their internal capabilities.
- The appeal of traditional EPP suites has somewhat been tempered over the recent years, with the emphasis and focus on newer malware detection features and capabilities such as machine learning and behavioral analysis. Still, many Type B and Type C organizations continue to derive significant value from the integration and common management provided by them.

Recommendations

Security and risk management leaders responsible for endpoint protection platforms:

- Type A organizations: Focus on solutions that are flexible and customizable to meet their operational requirements.

- Type B organizations: Focus on a blend of prevention and detection and response capabilities commensurate with the skills and experience of their security operations teams. Alternatively, evaluate MSS and MDR capabilities to extend their internally available capabilities.
- Type C organizations: Emphasize prevention-focused solutions. Evaluate EDR mainly as a forensics capability only, and favor solution providers that also offer MSS and MDR capabilities.

Strategic Planning Assumption

By 2021, endpoint protection platforms (EPPs) will provide automated, orchestrated incident investigation and breach response. Separate, stand-alone endpoint detection and response (EDR) solutions will focus on managed security service provider (MSSP) and large enterprise security operations center (SOC) environments.

What You Need to Know

This Critical Capabilities research is a continuation of the analysis for the 2018 Magic Quadrant for Endpoint Protection Platforms, and uses the same data collected during that research period.

In September 2017, in response to changing market dynamics and client requirements, Gartner adjusted its definition of an EPP. An EPP is a solution deployed on endpoint devices to prevent file-based malware, to detect and block malicious activity from trusted and untrusted applications, and to provide the investigation and remediation capabilities needed to dynamically respond to security incidents and alerts (see "Redefining Endpoint Protection for 2017 and 2018").

Organizations are placing a premium on protection and detection capabilities within an EPP, and are depreciating the EPP vendors' ability to provide data protection capabilities such as data loss prevention, encryption or server controls. Security buyers are increasingly looking to the built-in security capabilities of their OS vendors, and most organizations are adopting disk encryption at the OS level with BitLocker in Microsoft Windows 10 and FileVault in Apple macOS.

Concurrently, protection for servers has diverged from EPP, with specialized tools to address the modern hybrid data center (cloud and on-premises; see "Market Guide for Cloud Workload Protection Platforms"). Gartner recommends that organizations separate the purchasing decisions for server workloads from any product or strategy decisions involving endpoint protection. The evolutionary shift from hardware servers to virtual machines (VMs), containers and private/public cloud infrastructure means that server workloads now have different security requirements compared to end-user-focused, interactive endpoints (see "Endpoint and Server Security: Common Goals, Divergent Solutions").

This is a transformative period for the EPP market, and as the market has changed, so has the analysis profile used for this research. In the 2017 Magic Quadrant for Endpoint Protection Platforms, capabilities traditionally found in the EDR market (see "Market Guide for Endpoint Detection and Response Solutions") were considered as "nice to have" features. In this 2018

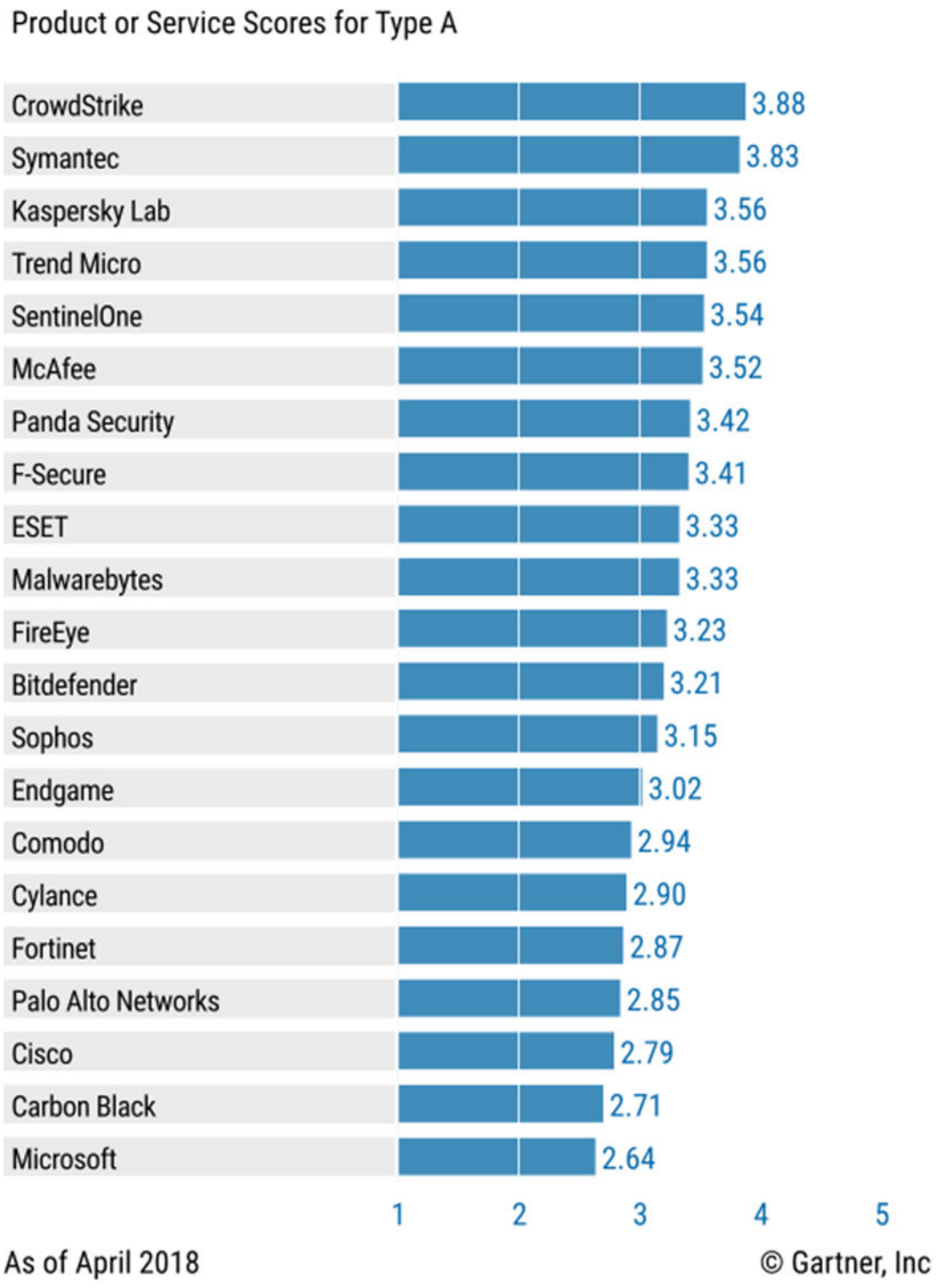
research, some of these features are now core components of an EPP that can address and respond to modern threats.

Note that definitions of Type A, B and C organizations are found in the Use Cases section.

Analysis

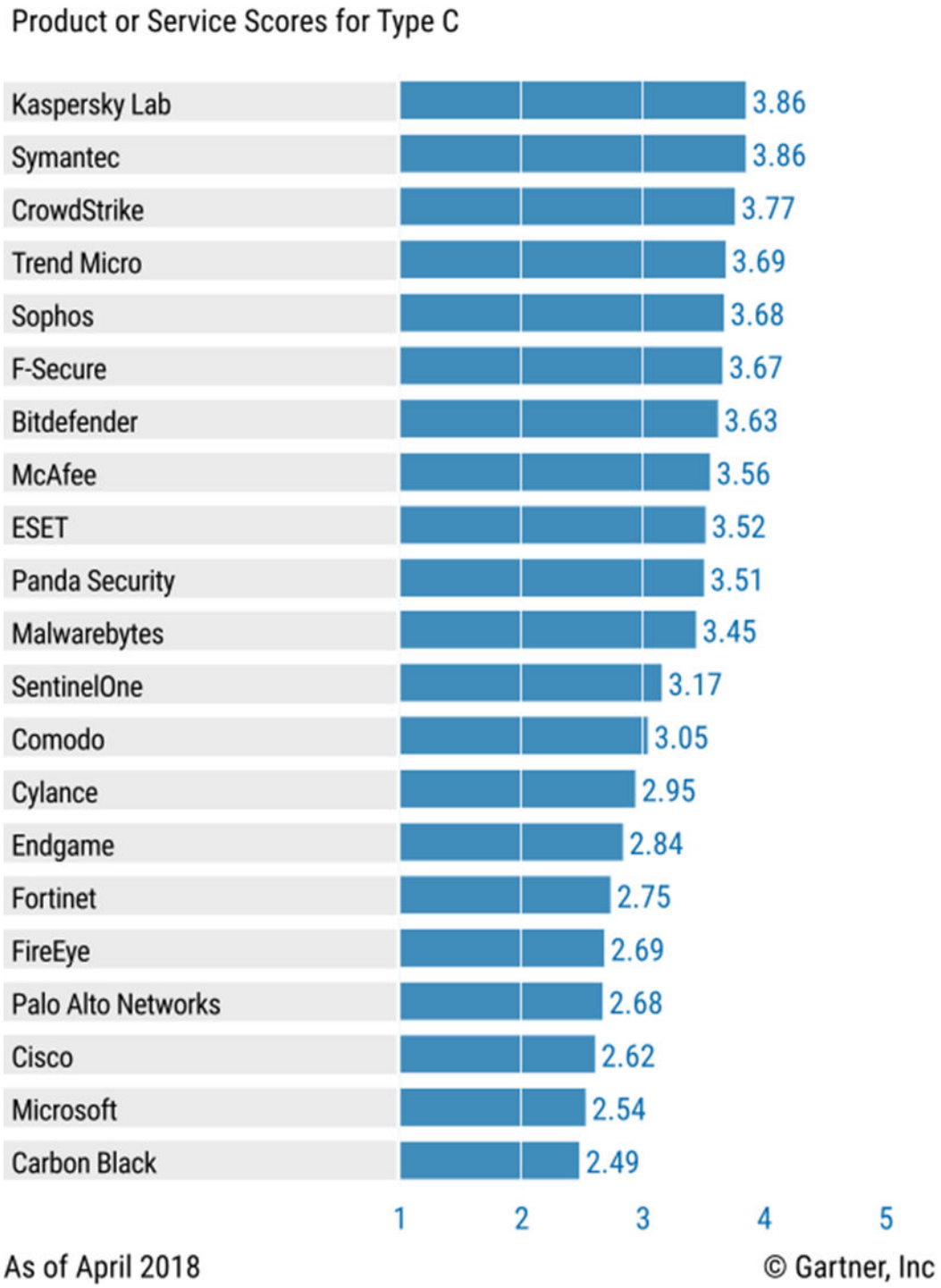
Critical Capabilities Use-Case Graphics

Figure 1. Vendors' Product Scores for Type A Use Case



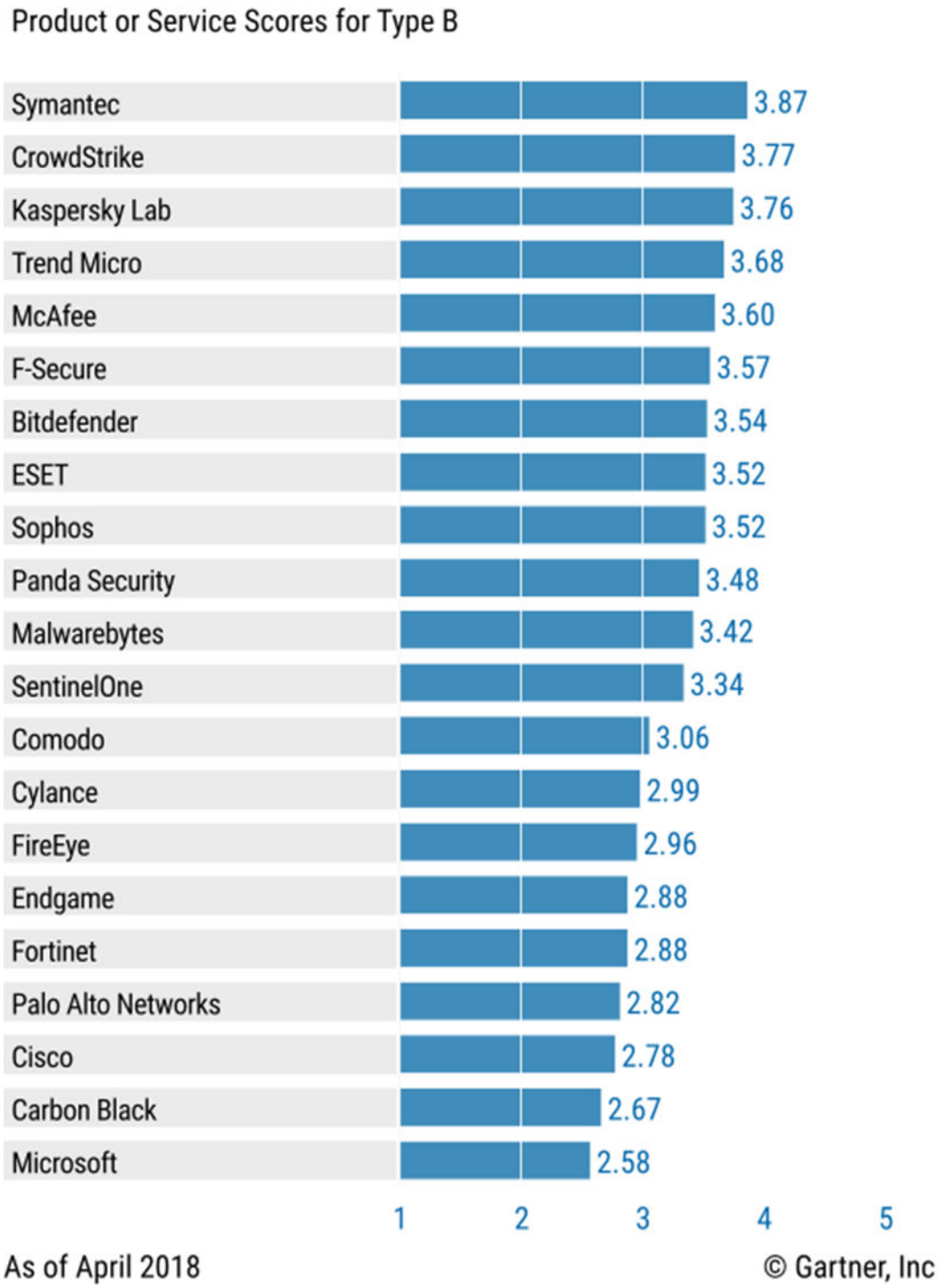
Source: Gartner (April 2018)

Figure 2. Vendors' Product Scores for Type B Use Case



Source: Gartner (April 2018)

Figure 3. Vendors' Product Scores for Type C Use Case



Source: Gartner (April 2018)

Vendors

Bitdefender

Bitdefender provides a solution that is among the highest evaluated effectiveness across a broad range of platforms and capabilities in third-party scores. Its solution is the most repackaged across all EPP vendors. Bitdefender offers EPP and EDR in one platform, and one agent across endpoints, and physical, virtual or cloud servers. While a large part of the installed base is in the consumer segment, the gap between enterprise and consumer business is narrowing.

Bitdefender is a good choice for organizations that value malware detection accuracy and performance, as well as full support for data center and cloud workloads from a single solution provider. Bitdefender is also a partner for Microsoft's Windows Defender Advanced Threat Protection (ATP) platform, providing agents for Linux and macOS.

The vendor continues to round out its endpoint features for larger enterprises. However, its brand awareness remains low. Bitdefender's cloud-based, single-agent approach, large installed base, and recently released EDR module keep it relevant in this space.

Carbon Black

Carbon Black is in the middle of a significant corporate transition, consolidating its overall offerings into a new cloud-based security platform called Predictive Security Cloud. The company's overall offerings consist of Cb Defense (EPP), Cb Response (threat hunting and incident response), and Cb Protection (application whitelisting and device lockdown). Carbon Black began to consolidate EDR features from Cb Response into Cb Defense in 2017 as it started to build a presence in the EPP market. With the upcoming movement to cloud-based management and agent consolidation, Carbon Black implementations should become much simpler for its clients.

Cb Response is typically found in more complex environments with very mature security operations teams. The Cb Defense agent collects and sends all the unfiltered endpoint data to the cloud using a proprietary data streaming mechanism that eliminates bursting and peaks on networks.

Cisco

Cisco's Advanced Malware Protection (AMP) for Endpoints consists of prevent, detect and respond capabilities deployed as a cloud-managed solution that can be hosted in a public or private cloud.

Cisco's AMP for Endpoints leverages similar technology to the AMP capabilities in other Cisco products. Its AMP Cloud technology detects known threats, and uses threat intelligence data from Threat Grid and Talos security researchers for exploit prevention.

Gartner clients rarely shortlist AMP for Endpoints for its technology. When they do, it is usually because they get a strong financial incentive when purchasing other Cisco products. AMP for Endpoints did not participate in public endpoint-focused third-party testing in 2017, which impacts its scores in this Critical Capabilities.

Cisco's AMP solution has the most appeal for existing Cisco clients that leverage other Cisco security solutions and aspire to establish security operations around Cisco products.

Comodo

The Comodo brand is best-known as a digital certificate authority. In October 2017, Francisco Partners acquired a majority stake in Comodo's certificate authority business, with Comodo planning to focus on its endpoint protection strategy.

Comodo Advanced Endpoint Protection (AEP) includes malware protection, a host-based intrusion prevention system (HIPS), web filtering, a personal firewall, sandbox analysis, vulnerability analysis and patching, and a classification capability that helps guarantee a good or bad verdict on all executable files. When an executable is untrusted or unknown, it is run in a tightly controlled container to isolate any potentially malicious activity.

Comodo also sells secure web gateways, web application firewalls and mobile device management focused on midsize enterprises and small and midsize businesses (SMBs). Its security products are managed from a central web-based portal that manages service request ticketing and workflow.

CrowdStrike

CrowdStrike Falcon's lightweight single agent supports all environments (physical, virtual and cloud) and functions with the same agent and management console for Falcon Prevent protection and Falcon Insight EDR. With its EDR heritage, CrowdStrike records most endpoint events and sends all recorded data to its cloud for analysis and detection. Some prevention is done locally on the agent.

Alongside EPP and EDR capabilities, CrowdStrike offers a complementary service called Falcon OverWatch that is widely used by its clients.

Falcon OverWatch provides managed threat hunting, alerting, response and investigation assistance.

Organizations with small or no SOC teams will find the combination of Falcon OverWatch and Falcon Endpoint Protection compelling. CrowdStrike also offers a well-respected breach response service.

Cylance

Cylance was one of the pioneers in using machine learning (ML) to detect file-based malware, but by 2017, most EPP competitors claimed to have added ML capabilities, pressuring Cylance to more aggressively address non-file-based attacks. In late May 2017, Cylance formally launched its EDR product, CylanceOPTICS, which was late to market compared to other vendors, and is generally perceived to be lacking in advanced capabilities already available in key competing products.

Eighty-five percent of Cylance's business is in North America, although the company has about 3,700 customers across the globe, half of which represent organizations with fewer than 500 seats.

CylancePROTECT is cloud-based, with Cylance hosting and managing the console infrastructure directly. The vendor finally started participating in the VirusTotal community in 2017, but has a poor third-party test participation record when compared with established EPP vendors.

Cylance is a good EPP shortlist candidate for organizations requiring a lightweight, low-impact client agent.

Endgame

Endgame is a privately held organization that has evolved from pure EDR for large enterprises and defense organizations, with the addition of prevention capabilities for the broader enterprise market.

Endgame is one of the few vendors in this analysis that sells a single product offering — meaning there are no additional add-ons or purchases — to address protection, detection and response use cases.

The platform is missing a number of traditional EPP-related features, such as application control and suspicious file quarantining. Yet Endgame scores well in protection capabilities by focusing on the tools, techniques and procedures used by adversaries, rather than simply looking for bad files.

Endgame's big differentiator is in its investigation and threat-hunting capabilities, where natural language understanding (NLU) queries, such as "Search for PowerShell" and "Find NetTraveler," allow organizations to make use of advanced detection capabilities without the need for deep experience.

Endgame is a good EPP shortlist candidate for organizations with an existing or emerging SOC where incident investigation and response is a key requirement.

ESET

ESET has a strong EPP market share among SMBs to large enterprises. It provides protection with a lightweight agent that includes a large protection stack, consisting of a host-based intrusion prevention system (HIPS), ML, exploit prevention, detection of in-memory attacks and ransomware behavior detection.

ESET recently launched an additional platform for EDR capabilities, called Enterprise Inspector. Customers with experienced security staff will be able to inspect and modify the detection rules within Enterprise Inspector, and further tailor them to their unique requirements.

ESET has significant security community mind share through published research, disruption of organized crime and its WeLiveSecurity website. The vendor's evaluation is impacted in this assessment by its limited cloud management capabilities, and the relative lateness of its EDR capabilities.

ESET has localized support in 35 languages, which means it is an attractive choice for globally distributed organizations. Its protection capabilities make it a solid shortlist candidate for any organization.

FireEye

FireEye is a security suite vendor that provides email, web, network, endpoint security and threat intelligence, which are managed in the Helix security operations platform.

FireEye revenue from its HX Series endpoint security product is a relatively small portion of the vendor's overall business. The HX management console is deployed through the cloud or as a virtual or on-premises hardware appliance that supports up to 100,000 endpoints.

FireEye Endpoint Security 4.0 shipped in late September 2017; therefore, market response to FireEye's endpoint protection capabilities was limited during this research period.

Fortinet

Fortinet is a network security suite vendor whose products include enterprise firewalls, email security, sandbox, web application firewalls and its FortiClient endpoint security software. FortiClient includes components designed to work in conjunction with Fortinet products, including FortiGate (firewall), FortiSandbox, FortiMail, FortiWeb and others.

FortiClient is not well-known to most Gartner clients that inquire about endpoint security, and we see little adoption of it outside of Fortinet's client base. FortiClient is becoming more focused on the enterprise space, but its current installed base is mostly in the SMB space, and about half of its customers have less than 1,000 seats installed.

Gartner clients will find Fortinet most appealing when integrated as part of an existing Fortinet deployment.

F-Secure

In 2017, F-Secure continued with its long track record for high-accuracy, lightweight and low-impact anti-malware detection with its cloud-based F-Secure Protection Service for Business (PSB) offering and on-premises solution, F-Secure Business Suite. F-Secure added an integrated password manager with password protection capabilities and improved device control management to PSB and Business Suite. F-Secure also added ML capabilities to Rapid Detection Service, which is its managed EDR solution.

Over the past 12 months, F-Secure further enhanced its product deployment and management capabilities, making it a good choice for larger, more complex enterprises.

F-Secure is focusing its investments in its managed service offerings, and has added product enhancements with a specific focus on preventing ransomware attacks.

Kaspersky Lab

Kaspersky Lab's research team makes up one-third of the organization, and is well-known for its accurate malware detection and in-depth investigation and analysis of many sophisticated attacks.

Kaspersky Lab is late to market with EDR capabilities, and has no vendor-managed, SaaS-type cloud-based management options for organizations with more than 1,000 endpoints to manage.

In September 2017, the U.S. government ordered all federal agencies to remove Kaspersky Lab's software from their systems. Furthermore, several media reports, citing unnamed intelligence sources, have claimed that Kaspersky's software was being used by the Russian government to access sensitive information. Although the U.S. government has not given any official explanation for the ban, Kaspersky Lab vehemently refutes the unsubstantiated claims and stresses that there has yet to be any evidence produced of its alleged wrongdoing. Kaspersky maintains that the actions lack sufficient basis and are unconstitutional, and has initiated legal action against the U.S. government. Gartner clients, especially those who work closely with U.S. federal agencies, should continue to monitor this situation for updates.

From a technology and malware prevention perspective, Kaspersky Lab remains a good candidate as a solution for any organization that is not constrained by U.S. government recommendations. Despite the media stories surrounding Kaspersky Lab, it continues to grow its endpoint presence globally.

Malwarebytes

In 2017, Malwarebytes delivered cloud-based management, and added mainstream and advanced EDR capabilities to its single agent, which includes the breach remediation tools for remediating infections. It is one of the few vendors in this space that can roll back the changes made by ransomware, including restoring files that were encrypted in the attack. This ransomware remediation can be performed remotely from the cloud management console up to 72 hours after the attack, without the need for any local access to an endpoint.

For organizations with small IT or security teams, Malwarebytes provides strong protection capabilities and some advanced EDR capabilities, all at an attractive price point. For larger organizations or organizations with a mature security team, there are some missing enterprise features that make the Malwarebytes solution a challenge to incorporate into an existing SOC workflow.

McAfee

Intel completed the sale of 51% McAfee to TPG in April 2017 and, as a stand-alone company, McAfee has refocused its efforts on the core aspect of its business: endpoint protection. McAfee remains one of the top three incumbent EPP vendors by market share, and its execution issues over the past three years make it the top competitive target for displacement by other vendors in the EPP Critical Capabilities.

Specifically, Endpoint Security (ENS) version 10.x (v.10.x) upgrades remained a very challenging adoption cycle for most McAfee clients. The feature set and protection capabilities included in the most recent release are quite compelling, and public test scores have improved over the past year. However, McAfee's execution assessment is hampered by organizations continuing to be hesitant to adopt the latest version, leaving those organizations vulnerable to commodity malware as well as

more advanced threats. Gartner client inquiry data identified McAfee as the single most-quoted EPP vendor that clients were planning to replace. Customer satisfaction scores were low again for 2017.

McAfee's ePolicy Orchestrator (ePO) continues to be the most quoted reason for clients initially adopting McAfee solutions in their environment, or for retaining McAfee over their contract terms and subsequent renewals. However, disenchantment with the EPP product is quickly eroding the perceived value of ePO in favor of vendors with cloud-based EPP management.

McAfee remains a good shortlist candidate for medium and larger organizations requiring an effective solution and that have a focus on an integrated management and reporting capability.

Microsoft

Microsoft is unique in the EPP space, as it is the only vendor with the capacity to embed protection features directly into the OS. It has used this advantage to step up its efforts in security with Windows 10 features, improvements to Windows Defender (also known as System Center EndpointProtection), and the addition of Windows Defender Advanced Threat Protection and Windows Defender Security Center.

Windows 10 OS-level features and capabilities available with Windows Enterprise E3 and E5, such as Application Guard, App Locker, Secure Boot, Device Guard, Exploit Guard, Advanced Threat Protection (ATP) and Credential Guard, significantly improve protection against current common threats. However, these protections are not as integrated in previous OS versions.

Overall, Microsoft now provides a broad range of security protections that address a wide spectrum of threats across endpoint, Office 365 and email. The comprehensive solution set will resonate with most organizations' security requirements, provided their budgets stretch to the higher-tier, E5-level subscription.

Microsoft has become the most-asked-about vendor during EPP-related Gartner client inquiry calls, and there is significant interest in using the security capabilities in Windows 10 to reduce security spend with other vendors. However, while it is improving its detection rates, the solution continues to be challenged to protect against sophisticated threats, and manageability of the solution remains a challenge.

Palo Alto Networks

Palo Alto Networks is still best-known to Gartner clients for its next-generation firewall (NGFW) product line, and this continues to be the main line of introduction to Palo Alto Networks Traps for Gartner clients.

Traps uses a stack of nonsignature detection capabilities, such as ML, static and dynamic analysis, as well as monitoring processes and applications as they are spawned for suspicious activity and events. Suspect files from the endpoint can be tested by Palo Alto Networks WildFire, its cloud-based threat analysis and malware sandboxing platform, which is included with a Traps subscription.

Palo Alto Networks acquired LightCyber in 2017; its behavioral-based analytics technology provides automated detection of suspicious user and entity activity indicative of malware. Traps without LightCyber currently offers limited EDR capabilities, which impacts its scores in this assessment.

Gartner clients will find Palo Alto Networks Traps most appealing when it can integrate with an existing Palo Alto Networks NGFW deployment.

Panda Security

Panda Security's main value proposition is the classification or attestation of every single executable file and process on a protected endpoint device. It is the only vendor to include a managed threat hunting service in the base purchase of its EPP. Adaptive Defense 360 is fully cloud managed, and combines EPP and EDR into a single offering and single agent.

The attestation service implements an automatic application whitelisting model, where only trusted and approved applications and processes are able to execute.

Panda Security's cloud-first approach, and the managed services backing the EPP and EDR capabilities, are beginning to increase brand awareness outside of Europe.

Organizations without experienced security staff will find Panda Security a good shortlist candidate for an EPP solution, as will organizations considering managed detection and response solutions that are prepared to replace their incumbent EPP vendor.

SentinelOne

SentinelOne is a part of the new wave of EPP solution providers that have experienced fast growth over the past few years. The cloud-based solution is designed around an embedded EDR feature set and behavioral protection. SentinelOne was one of the first vendors to offer a ransomware protection guarantee based on its behavioral detection and file journaling features.

SentinelOne offers endpoint visibility for investigative information in real time, and an API to integrate common-format, indicator of compromise (IOC)-based threat feeds.

SentinelOne is a good prospect to replace or augment existing EPP solutions for any organization looking for a solution with strong protection and visibility.

Sophos

In March 2017, Sophos acquired Invincea — a Visionary vendor in the 2017 Magic Quadrant for Endpoint Protection Platforms — giving Sophos access to its deep-learning ML algorithms.

The Sophos Intercept X product, designed to protect against and recover from the malicious actions related to ransomware and exploits, is available to Sophos Endpoint Protection customers and as an augmentation to an incumbent EPP.

Also included in the Intercept X purchase are Sophos' EDR-like capabilities — called Root Cause Analysis — and the ML malware detection technology from the acquisition of Invincea, which was added in late 2017.

Sophos' cloud-based EPP with the Intercept X platform is a good fit for organizations that can take advantage of a cloud-based administration platform, and that value strong protection against ransomware and exploit-based attacks over advanced forensic investigation capabilities.

Symantec

Symantec continues to provide one of the most comprehensive EPPs available in this market, with third-party test scores remaining in the top tier. Symantec has added advanced features to better address the changing threat landscape, becoming the first vendor to combine malware protection, EDR, system hardening and deception capabilities in a single agent. Application whitelisting continues to be a weak point.

Symantec has begun the process of migrating its offerings to a cloud-first model, with a hybrid option available to clients that prefer to maintain some of the management capabilities on-premises.

Symantec remains a good shortlist candidate for organizations of all sizes.

Trend Micro

Trend Micro is the third-largest vendor in the EPP market, with products ranging across network, data center and endpoint systems. It has a large worldwide footprint, with more than half of its business coming from Japan and the Americas.

Although the vendor has had a rather unremarkable year from a technology innovation perspective, it ticks boxes for mainstream EPP requirements, particularly for those looking for a comprehensive suite of solutions at an affordable price. Trend Micro's EDR solution is delivered as a separate agent to the EPP solution. While it integrates with additional on-premises products like the Deep Discovery sandbox, it lacks integration with its cloud sandbox, and cannot be managed from Trend Micro's cloud platform.

One of Trend Micro's biggest advantages is its vulnerability assessment and virtual patching technology, which uses an IPS engine to detect vulnerabilities, and uses HIPS to create a virtual patch to block the exploitation.

Trend Micro remains a good shortlist candidate for organizations of all sizes.

Context

When selecting EPP solutions, enterprises should evaluate them in terms of support for specific use cases. Vendors differ in their ability to accommodate different use cases. This research ranks vendors' solutions against typical use cases.

Product/Service Class Definition

Gartner reviewed the following classes of products and services: prevention, console alerting and reporting, EDR core functionality, EDR advanced response, third-party integration, EPP suite, managed services, geographic support, and OS support.

Critical Capabilities Definition

Prevention

This is the quality, quantity, accuracy and ease of administration of an EPP's anti-malware technology.

It covers the tools required to block file-based malware attacks, detect and prevent fileless malware attacks, and mitigate the risk of OS and application vulnerabilities. We look at test results from various independent testing organizations and data from VirusTotal, and use Gartner client inquiries as guides to the effectiveness of these techniques and implementations against modern malware.

EPP Suite

This is the support for EPP components traditionally offered as part of an extended EPP suite, in addition to anti-malware and anti-exploit based prevention.

These include offerings for a personal firewall, port and device control, application control, enterprise mobility management, data protection (such as full disk and file encryption) and data loss prevention. Vendors that offer a broad range of capabilities as part of an extended EPP suite are given extra credit here.

Console Alerting and Reporting

This is the provisioning of a centralized, role-centric console or dashboard that enhances the real-time visibility of an organization's endpoint security state.

It provides clearly prioritized alerts and warnings and intuitive administration workflows. Vendors that have delivered a cloud-first model with feature parity to an on-premises management platform are given extra credit, as organizations struggle to maintain visibility and control over endpoints in use by the increasing remote workforce.

EDR Core Functionality

This is the EDR component's capabilities for discovering, reporting and prioritizing vulnerabilities present in the environment.

It provides educated guidance for customers to visualize and investigate incidents, remediate malware infections and provide clear root cause analysis, helping reduce the attack surface. EDR core capabilities are typically focused on a forensics use of EDR, meaning investigating an event

well after it has occurred. Vendors that focus on lowering the knowledge and skills barrier through guided response tools and easy to-understand and easy-to-use user interfaces are given extra credit here.

EDR Advanced Response

These are the EDR component's advanced investigative and remediation capabilities, complex automation, and ability to send and receive detailed investigative workflow information.

It provides capabilities and customizations that push EDR from a functionally forensics-focused use case to an adaptable detection and response platform that can detect and investigate an event as it occurs. Vendors that focus on providing advanced customization capabilities required by an active security operations center are given extra credit here.

Third-Party Integration

This is the support via APIs, and unilateral and bidirectional integration of third-party on-premises and cloud-based solutions, such as Active Directory, security information and event management (SIEM), sandboxes, firewalls, threat and indicators of compromise feeds, and SOAR/orchestration.

It provides the ability to have unilateral and bilateral communications between the endpoint agent and/or console and third-party resources to enhance the prevention, detection, analysis and response capabilities with the rich data only available on these other platforms. Vendors that not only focus on providing a set of APIs for their own products, but that also have demonstrated integrations with a widely diverse set of third parties to provide additional context and correlation of events, are given extra credit here.

Managed Services

This is support for managed security solutions (MSS) and managed detection and response (MDR) offerings.

MSS offerings typically focus on the deployment and remote operation of traditional endpoint security solutions, including most of the components of a traditional EPP suite. MDR offerings focus on remotely delivering a managed security service that responds to threats that have made it past the prevention capabilities deployed within an environment. MDR solutions that actively detect, investigate, contain and mitigate threats are given extra credit here.

Geographic Support

This is a vendor's ability to support global customers, as well as the number of languages it supports.

Vendors offering local, regional support offices, 24/7 support in each client region, and other local resources to assist with the deployment and operation of their solutions in a global deployment context (including MSS and MDR) are given extra credit here.

OS Support

This is a vendor's ability to support the typical operating systems found in client organizations.

Several vendors focus solely on Windows endpoints. Solutions that can also support macOS and Linux with near parity on the features delivered in the Windows clients, most notably in advanced prevention and the activity and event monitoring areas of EDR, are given extra credit here.

Use Cases

Type A

Type A organizations, also referred to as "lean forward" organizations, adopt new technologies very early in the adoption cycle.

Type A organizations represent the smallest group of organizations. They have the budgeting and staffing resources to configure and implement new technologies and solutions rapidly within their environment. These organizations tend to focus on best-of-breed solutions that best address their business, technology and security needs and have the capacity to integrate, develop or build custom-made components as required. They see the use of technology as competitive differentiator. Their tolerance for risk is high and their approach to technology change is to run projects in parallel having multiple teams working on technology and business changes simultaneously. For EPP, these organizations focus on best-of-breed prevention, detection and response.

Type B

Type B organizations aim to stay relatively current on technology without getting too far ahead or behind their competition.

Type B organizations represent the largest group of organizations. They typically experience budgeting and staffing resource constraints and, as a result, focus on overall value by weighing the risks of the early use of new technology against the benefits. Their focus is on technology deployments that improve their organization's productivity, product quality, customer service and security. Type B organizations typically wait for a technology to become mainstream before considering implementation. They tend to be moderate in their approach, frequently using benchmarks within their industry to justify their investments in technology. Type B organizations balance innovation with reasonable caution when selecting new solutions. For EPP, these organizations focus on a blended approach between prevention, detection and response capabilities that can be complimented with managed services where needed.

Type C

Type C organizations typically view technology as an expense or operational necessity, and use it as a means to reduce costs.

Type C organizations represent the second-largest group. These organizations experience severe budgeting and staffing resource constraints and, as a result, prefer simply to deploy and use integrated solutions with managed services add-ons that can best complement their minimal staff. These organizations wait for technologies to become absolutely stable and for costs to acquire and operate to reach the lowest quartile before committing to purchase. For EPP, these organizations focus on prevention, rather than on integrated detection and response capabilities and solutions that offer a complement of managed services.

Vendors Added and Dropped

Added

None

Dropped

None

Inclusion Criteria

Inclusion in this Critical Capabilities was limited to vendors that met these minimum criteria:

- The majority of detection events must be from the vendor's own detection technique, and designed, owned and maintained by the vendor itself. Augmenting with an OEM engine is acceptable, provided it is not the primary method of detection.
- The vendor's nonconsumer EPP must have participated in independent, well-known, public tests for accuracy and effectiveness within the 12 months prior to 18 November 2017, or be a current participant in the VirusTotal public interface. Examples include Virus Bulletin, AV-TEST, AV-Comparatives, NSS Labs and SE Labs.
- The vendor must have more than five named accounts larger than 10,000 seats that use the vendor's EPP as their sole EPP.
- The vendor must have a minimum of 500,000 deployed licenses, protecting nonconsumer endpoints, with at least 50,000 of those licenses protecting nonconsumer endpoints within North America.
- The vendor must satisfy at least 12 of the following "basic" capabilities, and at least four of the following "desirable" capabilities:
    - Basic capabilities:
        - Blocks known and unknown file-based malware, without relying on daily signature distribution
        - Detects suspicious and malicious activity based on the behavior of a process

- Implements protection for common application vulnerabilities and memory exploit techniques
- Can perform static, on-demand malware detection scans of folders, drives or devices such as USB drives
- Suspicious event data can be stored in a centralized location for retrospective IOC and indicator of attack (IOA) searching and analysis
- Allows real-time IOC/IOA searching across all endpoints (for example, file hash, source/destination IP, registry key)
- Allows remote quarantining of an endpoint, restricting network access to only the EPP management server
- Automatically updates policies, controls and new agent/engine versions without connecting directly to the corporate network
- Continues to collect suspicious event data when outside of the corporate network
- Detections and alerts include severity and confidence indicators, to aid in prioritization
- Provides risk-prioritized views based on confidence of the verdict and severity of the incident
- Displays full process tree to identify how processes were spawned, for an actionable root cause analysis
- Automatically quarantines malicious files
- Identifies changes made by malware, and provides the recommended remediation steps
- Detects, blocks and reports attempt to disable or remove the EPP agent

- Desirable capabilities:
  - Primary EPP console uses a cloud-based, SaaS-style, multitenant infrastructure, and is operated, managed and maintained by the vendor
  - Implements vulnerability shielding (aka virtual patching) for known vulnerabilities in the OS and for non-OS applications
  - Can implement default-deny whitelisting with a vendor-maintained "app store"-type approach and user self-service features
  - Can implement application isolation to separate untrusted applications from the rest of the system
  - Includes access to a cloud- or network-based sandbox that is VM-evasion-aware
  - Includes deception capabilities designed to expose an attacker

- Vendor itself offers managed detection services, alerting customers to suspicious activity
- Vendor itself offers managed threat hunting, or managed IOC/IOA searching, for detecting the existence of threats (not via a third party or channel)
- Supports advanced natural-language queries with operators and thresholds (for example, "Show all machines with new PE >1 week old AND on <2% of Machines OR Unknown")
- Provides guided analysis and remediation based on intelligence gathered by the vendor (for example, "85% of organizations follow these steps")
- Provides attribution information and potential motivations behind attacks
- Can utilize third-party, community and intelligence feeds
- Allows remote remediation via the management console
- Includes APIs for integration with security orchestration, automation and response (SOAR)/orchestration for automation

Table 1. Weighting for Critical Capabilities in Use Cases

Critical Capabilities	Type A	Type B	Type C
Prevention	10%	15%	20%
Console Alerting and Reporting	5%	15%	20%
EDR Core Functionality	20%	15%	10%
EDR Advanced Response	20%	5%	0%
Third-Party Integration	15%	5%	0%
EPP Suite	5%	10%	15%
Managed Services	5%	15%	25%
Geographic Support	10%	10%	5%
OS Support	10%	10%	5%
Total	100%	100%	100%

Source: Gartner (April 2018)

This methodology requires analysts to identify the critical capabilities for a class of products/ services. Each capability is then weighed in terms of its relative importance for specific product/ service use cases.

Critical Capabilities Rating

Each of the products/services has been evaluated on the critical capabilities on a scale of 1 to 5; a score of 1 = Poor (most or all defined requirements are not achieved), while 5 = Outstanding (significantly exceeds requirements).

Table 2. Product/Service Rating on Critical Capabilities

Critical Capabilities	Bitdefender	Carbon Black	Cisco	Comodo	CrowdStrike	Cylance	Endgame	ESET	FireEye	Fortinet	F-Secure	Kaspersky Lab	Malwarebytes	McAfee	Microsoft	Palo Alto Networks	Panda Security	SentinelOne	Sophos	Symantec	Trend Micro
Prevention	4.5	2.3	2.3	3.5	3.5	3.0	3.7	4.5	2.3	2.5	4.0	4.8	4.5	4.0	3.0	3.5	4.0	3.7	4.3	4.5	4.5
Console Alerting and Report-ing	3.5	3.0	3.0	3.0	4.0	3.0	3.5	4.0	3.0	2.8	3.5	3.8	4.0	4.3	2.2	3.0	3.3	3.5	4.0	4.0	3.8
EDR Core Functionality	2.5	3.0	3.0	2.5	4.0	3.0	4.0	3.3	3.5	3.0	4.0	3.2	3.5	3.3	3.0	2.8	3.8	3.8	2.5	3.8	3.3
EDR Advanced Response	2.0	2.0	2.2	3.0	4.5	2.2	3.5	2.8	3.5	2.5	3.2	3.2	3.3	3.2	2.5	2.0	3.2	3.8	2.5	3.8	3.2
Third-Party Integration	3.2	3.0	3.0	2.0	4.0	3.0	2.5	2.5	3.3	2.5	2.5	3.0	2.5	3.3	2.5	3.5	3.0	3.5	2.5	3.3	3.2
EPP Suite	4.0	1.0	1.0	3.0	2.0	2.0	2.0	4.0	1.0	3.5	3.8	4.5	3.8	4.5	3.0	1.7	3.0	2.5	4.5	4.5	4.5
Managed Services	3.0	2.5	3.0	2.7	4.9	3.2	2.0	2.0	3.0	2.0	3.5	3.0	2.0	2.0	2.0	2.0	3.5	2.5	2.8	2.8	2.5
Geographic Support	4.0	4.0	4.0	3.7	3.0	3.5	2.0	4.0	4.0	3.8	3.0	4.0	4.0	4.0	4.0	4.0	3.0	3.0	4.0	4.0	4.1
OS Support	4.5	3.0	3.2	3.8	3.8	3.5	2.0	3.8	3.5	3.5	3.5	3.8	2.5	3.8	1.0	2.8	3.8	4.0	3.8	4.0	3.8

Source: Gartner (April 2018)

Table 3 shows the product/service scores for each use case. The scores, which are generated by multiplying the use case weightings by the product/service ratings, summarize how well the critical capabilities are met for each use case.

Table 3. Product Score in Use Cases

Use Cases	Bitdefender	Carbon Black	Cisco	Comodo	CrowdStrike	Cylance	Endgame	ESET	FireEye	Fortinet	F-Secure	Kaspersky Lab	Malwarebytes	McAfee	Microsoft	Palo Alto Networks	Panda Security	SentinelOne	Sophos	Symantec	Trend Micro
Type A	3.21	2.71	2.79	2.94	3.88	2.90	3.02	3.33	3.23	2.87	3.41	3.56	3.33	3.52	2.64	2.85	3.42	3.54	3.15	3.83	3.56
Type B	3.54	2.67	2.78	3.06	3.77	2.99	2.88	3.52	2.96	2.88	3.57	3.76	3.42	3.60	2.58	2.82	3.48	3.34	3.52	3.87	3.68
Type C	3.63	2.49	2.62	3.05	3.77	2.95	2.84	3.52	2.69	2.75	3.67	3.86	3.45	3.56	2.54	2.68	3.51	3.17	3.68	3.86	3.69

Source: Gartner (April 2018)

To determine an overall score for each product/service in the use cases, multiply the ratings in Table 2 by the weightings shown in Table 1.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"How Products and Services Are Evaluated in Gartner Critical Capabilities"

"Magic Quadrant for Endpoint Protection Platforms"

Evidence

- Gartner responded to more than 2,100 client inquiries from 1Q17 to 1Q18.
- Gartner conducted an online survey of 129 EPP reference customers in 4Q17.
- Gartner conducted an online survey of 55 EPP channel references in 4Q17.

Critical Capabilities Methodology

This methodology requires analysts to identify the critical capabilities for a class of products or services. Each capability is then weighted in terms of its relative importance for specific product or service use cases. Next, products/services are rated in terms of how well they achieve each of the critical capabilities. A score that summarizes how well they meet the critical capabilities for each use case is then calculated for each product/service.

"Critical capabilities" are attributes that differentiate products/services in a class in terms of their quality and performance. Gartner recommends that users consider the set of critical capabilities as some of the most important criteria for acquisition decisions.

In defining the product/service category for evaluation, the analyst first identifies the leading uses for the products/services in this market. What needs are end-users looking to fulfill, when considering products/services in this market? Use cases should match common client deployment scenarios. These distinct client scenarios define the Use Cases.

The analyst then identifies the critical capabilities. These capabilities are generalized groups of features commonly required by this class of products/services. Each capability is assigned a level of importance in fulfilling that particular need; some sets of features are more important than others, depending on the use case being evaluated.

Each vendor's product or service is evaluated in terms of how well it delivers each capability, on a five-point scale. These ratings are displayed side-by-side for all vendors, allowing easy comparisons between the different sets of features.

Ratings and summary scores range from 1.0 to 5.0:

1 = Poor or Absent: most or all defined requirements for a capability are not achieved

2 = Fair: some requirements are not achieved

3 = Good: meets requirements

4 = Excellent: meets or exceeds some requirements

5 = Outstanding: significantly exceeds requirements

To determine an overall score for each product in the use cases, the product ratings are multiplied by the weightings to come up with the product score in use cases.

The critical capabilities Gartner has selected do not represent all capabilities for any product; therefore, may not represent those most important for a specific use situation or business objective. Clients should use a critical capabilities analysis as one of several sources of input about a product before making a product/service decision.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp

NuHarbor Security
39 River Road, Suite 4
Essex Junction,, VT 05452 US
(800) 917-5719
finance@nuharborsecurity.com
www.nuharborsecurity.com

Invoice

BILL TO

New Hampshire Sectretary of State
Attn: Paula Penney
State House, Room 204
107 Main Street
Concord, NH 03301-4989

INVOICE # NHSOS-0619-02
DATE 06/14/2019
DUE DATE 07/14/2019
TERMS Net 30

PO
NHSOS-19-SW59

DESCRIPTION	QUANTITY	RATE	AMOUNT
CS-FCSD-SOLN-T2 - Falcon Complete Advanced Next-Generation Antivirus (Prevent) + Endpoint Detection & Response (Insight) + IT Hygiene (Discover) Falcon Complete Subscription Included. List Price 275.75 (per endpoint) Discounted Price 118.65 (per endpoint)	370	118.65	43,900.50
CS-OW-SVC-T3 - Falcon Overwatch Service - 24x7x365 Managed Hunting - Team Included in Falcon Complete	370	0.00	0.00T
CS-PE-07 - Threat Graph Standard -- Standard Retention (7 Day) - Included in Falcon Complete	370	0.00	0.00T
CS-Device-SO:M-T3 - Falcon Device Control - Removeable Media Control - List Price 9.6 Discounted Price 1.54	370	1.54	569.80T

Thank you for the opportunity to work with the NH Secretary of State on this project.

SUBTOTAL	44,470.30
TAX (0%)	0.00
TOTAL	44,470.30
BALANCE DUE	**$44,470.30**

NuHarbor SECURITY

QUOTE

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE	June 15, 2018
QUOTE EXPIRES	July 15, 2018
TERMS	Net 30

TO: Daniel Cloutier
Assistant Secretary of State
State of New Hampshire
71 South Fruit Street
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Chief Financial Officer
NuHarbor Security
PO Box 51958
Boston MA 02205
finance@nuharborsecurity.com
(802) 448-4483

Software, Support, and Implementation

Line No.	Part No.	Description	Unit Price	Qty	Amount
1	CS-EPPADV-SOLN-T3	EPP Advanced (Prevent + Insight + Discover) - Band 3	23.23	370.00	8,595.10
2	CS-OW-SVC-T3	Falcon Overwatch Service - Band 3	6.35	370.00	2,349.50
3	CS-PE-07	Falcon Platform - Standard Retention (7 Day)	6.72	370.00	2,486.40
4	CS-EPPCOMP-SOLN	EPP Complete	78.43	370.00	29,019.10
5	CS-DEVICE-SOLN	Falcon Device Control	2.12	370.00	784.40
				TOTAL	**$43,234.50**

NuHarbor SECURITY

QUOTE

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE	July 19, 2018
QUOTE EXPIRES	August 18, 2018
TERMS	Net 30

TO: Daniel Cloutier
Assistant Secretary of State
State of New Hampshire
71 South Fruit Street
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Chief Financial Officer
NuHarbor Security
PO Box 51958
Boston MA 02205
finance@nuharborsecurity.com
(802) 448-4483

Software, Support, and Implementation

Line No.	Part No.	Description	List Price	Unit Price	Qty	Amount
1	CS-EPPADV-SOLN-T3	EPP Advanced (Prevent + Insight + Discover) - Band 3	97.16	23.23	370.00	8,595.10
2	CS-OW-SVC-T3	Falcon Overwatch Service - Band 3	25.91	6.35	370.00	2,349.50
3	CS-PE-07	Falcon Platform - Standard Retention (7 Day)	6.72	6.72	370.00	2,486.40
4	CS-EPPCOMP-SOLN	EPP Complete	82.65	78.43	370.00	29,019.10
5	CS-DEVICE-SOLN	Falcon Device Control	9.96	2.12	370.00	784.40
		LIST TOTAL	**$ 82,288.00**		**TOTAL**	**$ 43,234.50**

NuHarbor SECURITY

CROWDSTRIKE

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE May 7, 2019
QUOTE EXPIRES June 6, 2019

TO: Daniel Cloutier
Assistant Secretary of State, Director of IT & Data Security
State of New Hampshire
9 Ratification Way
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
finance@nuharborsecurity.com
(802) 448-4483

Software & Services Renewal

Line No.	Part No.	Description	List Price (per endpoint)	Discounted Price (per endpoint)	Qty	Amount
1	CS-FCSD-SOLN-T2	**Falcon Complete** Advanced Next-Generation Antivirus (Prevent) + Endpoint Detection & Response (Insight) + IT Hygiene (Discover) *Falcon Complete Subscription Included*	275.75	118.65	370.00	43,900.50
2	CS-OW-SVC-T3	**Falcon Overwatch Service** 24x7x365 Managed Hunting Team *Included in Falcon Complete*	-	-	370.00	-
3	CS-PE-07	**Threat Graph Standard** Standard Retention (7 Day) *Included in Falcon Complete*	-	-	370.00	-
4	CS-DEVICE-SOLN-T3	**Falcon Device Control** Removeable Media Control	9.96	1.54	370.00	569.80
		LIST TOTAL	**$ 102,407.46**		**TOTAL**	**$ 44,470.30**

12 Month Term Licensing

NuHarbor Security Terms:
Invoice for this purchase shall occur upon Client receiving deliverable. Invoice payments are due net thirty (30) days from date of invoice. Accounts not paid within these terms are subject to a 1% monthly finance charge.
If applicable, Client is responsible for all state sales tax
The Subscription Start Date shall be the date this Order is fully executed.
Once executed by The Bill to Account, this Order is non-cancellable and amounts paid are non-refundable.
Client agrees to the terms and total set forth herein as indicated by the signatures and date of their respective duly authorized representatives below:

Signature

Print Name

Title

Date

NuHarbor SECURITY

proofpoint

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE April 29, 2019
QUOTE EXPIRES June 15, 2019

TO: Daniel Cloutier
Assistant Secretary of State
State of New Hampshire
71 South Fruit Street
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
finance@nuharborsecurity.com
(802) 448-4483

Software & Support Renewal

Line No.	Part No.	Description	Unit Price	Qty	Amount
1	PP-B-TBEPF-S-A-101	TAP URL Defense & AttDef, TAP Dashboard, Dynamic Reputation, Spam, Virus Protection, Zero-Hour Anti-Virus, Email Firewall, Impostor email, greymail filtering, Smart Search - F-Secure - SaaS 1-250, 12 Months 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	19,687.50	1.00	19,687.50
2	PP-SUP-PS-SME-12	Platinum Level Support - SME - 12 months support 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	0.00	1.00	0.00
				TOTAL	**$19,687.50**

12 Month Term Licensing

NuHarbor Security Terms:
Invoice for this purchase shall occur upon Client receiving deliverable. Invoice payments are due net thirty (30) days from date of invoice. Accounts not paid within these terms are subject to a 1% monthly finance charge.
If applicable, Client is responsible for all state sales tax
The Subscription Start Date shall be the date this Order is fully executed.
Once executed by The Bill to Account, this Order is non-cancellable and amounts paid are non-refundable.
Client agrees to the terms and total set forth herein as indicated by the signatures and date of their respective duly authorized representatives below:

Signature

Print Name

Title

Date

NuHarbor SECURITY

proofpoint

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE June 12, 2019
QUOTE EXPIRES June 15, 2019

TO: Daniel Cloutier
Assistant Secretary of State, Director of IT & Data Security
State of New Hampshire
71 South Fruit Street
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Finance Department
NuHarbor Security
39 River Road
Essex Junction, VT 05452
finance@nuharborsecurity.com
(802) 448-4483

Software & Support Renewal / Upgrade

Line No.	Part No.	Description	Unit Price	Qty	Amount
1	PP-B-TBEPF-S-A-101	TAP URL Defense & AttDef, TAP Dashboard, Dynamic Reputation, Spam, Virus Protection, Zero-Hour Anti-Virus, Email Firewall, Impostor email, greymail filtering, Smart Search - F-Secure - SaaS 1-250, 12 Months 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	19,687.50	1.00	19,687.50
2	PP-SUP-PS-SME-12	Platinum Level Support - SME - 12 months support 125 Users Start Date: 06/26/2019 End Date: 06/25/2020	0.00	1.00	0.00
3	PP-M-AP-V-B-101	PFPT Threat Response Auto-Pull (AP) Tier 1 - Up to 125 Users	4,150.00	1.00	4,150.00
4	PP-PST-PTR-A-101	PFPT Configuration - Threat Response	-	1.00	-
5	PP-SUP-PS-S-12	Platinum Level Support - SaaS (Included) - 12 months support 125 Users	0.00	1.00	0.00
				TOTAL	**$23,837.50**

12 Month Term Licensing

NuHarbor Security Terms:
Invoice for this purchase shall occur upon Client receiving deliverable. Invoice payments are due net thirty (30) days from date of invoice. Accounts not paid within these terms are subject to a 1% monthly finance charge.
If applicable, Client is responsible for all state sales tax
The Subscription Start Date shall be the date this Order is fully executed.
Once executed by The Bill to Account, this Order is non-cancellable and amounts paid are non-refundable.
Client agrees to the terms and total set forth herein as indicated by the signatures and date of their respective duly authorized representatives below:

Signature

Print Name

Title

Date

State of New Hampshire
Department of State

Chief Financial Officer
NuHarbor Security
PO Box 51958
Boston, MA 02205
1-802-448-4483

July 24, 2018

Description: PO # NHSOS-19-SW04	Qty	Price	Total
CS-EPPADV-SOLN-T3 | EPP Advanced (Prevent + Insight + Discover) – Band 3	370	23.23	$ 8,595.10
CS-OW-SVC-T3 | Falcon Overwatch Service – Band 3	370	6.35	2,349.50
CS-PE-07 | Falcon Platform – Standard Retention (7 Day)	370	6.72	2.486.40
CS-EPPCOMP-SOLN | EPP Complete	370	78.43	29,019.10
CS-DEVICE-SOLN | Falcon Device Control	370	2.12	784.40
Total Quote for this PO (See Attached Quote and Document References)			**$43,234.50**

Bill To: (send 2 copies of the invoice please):

New Hampshire Secretary of State
Attn: Paula Penney
State House, Room 204
107 North Main Street
Concord, NH, 03301-4989
Telephone: (603) 271-3242

Ship To:

New Hampshire Secretary of State
Attn: Daniel J. Cloutier
9 Ratification Way
(formerly 71 S Fruit St)
Concord, NH, 03301

Order Contact: Daniel J. Cloutier, Assistant Secretary of State, eMail: Daniel.Cloutier@sos.nh.gov, 1-603-271-0001

Use the name "NH Secretary of State" on all license agreements or other documents as required.

Sincerely,

David M. Scanlan
Deputy Secretary of State

Date 7/24/2018

NuHarbor SECURITY

QUOTE

39 River Road
Suite 4
Essex Junction, VT 05452

QUOTE DATE	July 19, 2018
QUOTE EXPIRES	August 18, 2018
TERMS	Net 30

TO: Daniel Cloutier
Assistant Secretary of State
State of New Hampshire
71 South Fruit Street
Concord, NH 03301
daniel.cloutier@sos.nh.gov
(603) 271-0001

ADDRESS CORRESPONDENCE TO:
Chief Financial Officer
NuHarbor Security
PO Box 51958
Boston MA 02205
finance@nuharborsecurity.com
(802) 448-4483

Software, Support, and Implementation

Line No.	Part No.	Description	List Price	Unit Price	Qty	Amount
1	CS-EPPADV-SOLN-T3	EPP Advanced (Prevent + Insight + Discover) - Band 3	97.16	23.23	370.00	8,595.10
2	CS-OW-SVC-T3	Falcon Overwatch Service - Band 3	25.91	6.35	370.00	2,349.50
3	CS-PE-07	Falcon Platform - Standard Retention (7 Day)	6.72	6.72	370.00	2,486.40
4	CS-EPPCOMP-SOLN	EPP Complete	82.65	78.43	370.00	29,019.10
5	CS-DEVICE-SOLN	Falcon Device Control	9.96	2.12	370.00	784.40
		LIST TOTAL	**$ 82,288.00**		**TOTAL**	**$ 43,234.50**

CROWDSTRIKE

FALCON ENDPOINT PROTECTION **COMPLETE**™

A REVOLUTIONARY APPROACH TO ENDPOINT SECURITY

Complete endpoint security with unrivaled simplicity — guaranteed

FALCON ENDPOINT PROTECTION COMPLETE — TURNKEY ENDPOINT SECURITY THAT INCLUDES THE ONLY BREACH PREVENTION WARRANTY OF ITS KIND

A truly effective endpoint security solution requires a holistic approach. However, many organizations struggle to implement a comprehensive program because the time, cost and expertise needed are too high.

Falcon Endpoint Protection (EPP) Complete™ solves this problem by adding a team of security experts to handle every aspect of CrowdStrike® endpoint security technology for you. This powerful combination of people, processes and technology brings you to the highest level of endpoint security maturity without the burden of building it yourself. Falcon EPP Complete™ includes:

FALCON EPP COMPLETE™ SOLUTIONS

- **Falcon Prevent™** — next-gen antivirus with machine learning, exploit blocking, indicator of attack (IOA) behavioral analysis and more
- **Falcon Insight™** — endpoint detection and response (EDR)
- **Falcon Discover™** — IT hygiene and asset inventory
- **Falcon OverWatch™** — 24/7 managed threat hunting with managed detection and response (MDR)

FALCON EPP COMPLETE™ TEAM

- On-boarding
- Proactive configuration management
- Prevention health checks
- Maintenance and operations
- Incident handling playbook
- Incident triage and handling
- Hands-on remote remediation

TAKING ENDPOINT SECURITY TO THE NEXT LEVEL — THE BEST PROTECTION, 100 PERCENT MANAGED AND WORRY-FREE

Falcon EPP Complete provides the products and a seasoned team of experts to perform the tasks needed to handle all aspects of endpoint security, freeing you and your teams to focus on other important aspects of your business.

KEY BENEFITS

» Includes an exclusive warranty, for ultimate peace of mind

» Eliminates endpoint security burdens, providing effortless implementation, operations and incident remediation

» Provides remote remediation for timely, hassle-free incident resolution

» Offers the simplest and most effective endpoint security solution, accessible to all: Buy it and forget it

» Delivers immediate response and remediation anywhere

» Protects above and beyond traditional antivirus and other next-gen products

INCLUDES A BREACH PROTECTION WARRANTY OF UP TO $1 MILLION

In addition, Falcon EPP Complete is covered by a breach prevention warranty for the duration of the product subscription. The warranty provides up to $1 million of coverage to address any breach that occurs within the protected environment.

KEY PRODUCT CAPABILITIES

Falcon EPP Complete™ provides all the technologies and services required to instantly implement and continuously run a mature endpoint security program. It delivers the following benefits:

UNMATCHED NEXT-GEN EPP BENEFITS'

- **Guarantees protection:** Falcon EPP Complete comes with a breach protection warranty that covers the costs you would incur in responding to a breach, including legal services, client notification, identity theft and credit monitoring, forensics investigation and public relations.
- **Protects against all types of attacks:** Falcon EPP Complete™ protects your organization against commodity and zero-day malware, ransomware, exploits and advanced malware-free, fileless attacks — keeping you ahead of the rapidly changing tactics, techniques and procedures (TTPs) used by today's adversaries.
- **Combines the best prevention technologies:** For ultimate protection, Falcon EPP Complete™ combines technologies such as machine learning for malware protection, indicator of attack (IOA) behavioral blocking and exploit blocking.
- **Single, lightweight agent:** Falcon EPP Complete™ uniquely integrates powerful best-in-class prevention, detection and response, together with IT hygiene capabilities to provide continuous breach prevention in a single agent.

A FORCE MULTIPLIER: ALL THE HANDS-ON HELP AND EXPERTISE YOU NEED, WHEN YOU NEED IT

- **Gets you up and running and fully operational —** The Falcon EPP Team works with your organization to get you started and assists your team throughout the deployment process. During this interactive phase, CrowdStrike helps you understand the prevention capabilities of the Falcon platform and tailors these security postures to best fit your business and security needs.
- **Frees your IT and security teams from daily, time-consuming endpoint security tasks —** After initial implementation, the Falcon EPP Team administers the updates and maintenance of your solution, updating, monitoring and tuning Falcon to continually enhance your security posture. The team also reviews, triages, prioritizes and resolves alerts generated by the Falcon platform and Falcon OverWatch. The team identifies whether an alert is a false positive or a true incident and responds accordingly.
- **Reduces risk with immediate remote remediation of incidents —** When the Falcon EPP Team detects an incident, it can remotely remediate it. By ensuring that all incidents are handled immediately, Falcon EPP Complete™ dramatically reduces the risks of a serious breach. In addition, the Falcon EPP Team assists with guidance and expertise to help your teams with any security concerns they might have.

IMMEDIATE TIME-TO-VALUE

- **Easy deployment —** As part of the CrowdStrike platform, Falcon EPP Complete™ requires only the installation of a small 25 MB agent, without requiring management infrastructure or management consoles, making deployment easy and efficient.
- **Immediately operational —** Falcon EPP Complete™ can be deployed instantly for unrivaled time-to-value. As soon as it's installed, it hits the ground running, allowing the Falcon EPP Team to monitor and protect your organization without requiring additional components, reboots, query writing, staging or complex configuration.
- **Zero impact on performance —** Thanks to its cloud-native architecture, Falcon EPP Complete causes no additional impact on endpoints or the network.

ENDPOINT SECURITY AT ITS BEST

Falcon Endpoint Protection (EPP) Complete™ revolutionizes endpoint security by providing all of the components required for a mature endpoint security posture, from the initial setup and day-to-day operations to the prevention and detection of threats, all the way to full incident handling, including immediate remote remediation and recovery.

FALCON EPP COMPLETE: A UNIQUE SOLUTION

CrowdStrike Falcon EPP Complete™ is the only endpoint security solution with built-in proactive threat hunting and remote remediation, backed by a team of security experts that serves as your force multiplier, 24/7.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR), IT hygiene, vulnerability management and a 24/7 managed hunting service — all delivered via a single lightweight agent.

Learn more at **crowdstrike.com**

CROWDSTRIKE

CROWDSTRIKE FALCON DEVICE CONTROL

Ensures safe device usage, extensive visibility and granular control: the industry's only cloud-delivered device control solution

CROWDSTRIKE FALCON DEVICE CONTROL

ENSURING SAFE AND ACCOUNTABLE DEVICE USAGE

The portability and usability of USB devices make them essential in today's enterprise environments. Yet these devices pose a significant security risk, bringing malware into organizations and leaking data out. Although device control solutions exist, they don't provide the contextual visibility and granular control required to understand and manage today's powerful devices.

Falcon Device Control™ ensures the safe utilization of USB devices across your organization. Built on the Falcon platform, it uniquely combines extensive visibility and granular control, allowing administrators to ensure that only approved devices are used in your environment. It also provides real-time and historical visibility, including detailed logging and reporting capabilities, giving you a complete understanding of device usage and files written to devices.

Leveraging the power of the CrowdStrike® platform and accessed through the Falcon management console, Falcon Device Control is the industry's only 100 percent cloud-delivered and managed device control solution.

KEY BENEFITS

- Mitigate risks associated with USB devices
- Gain automatic and complete visibility on USB device usage
- Control device usage with precision
- Implement and manage policies without hassle

KEY PRODUCT CAPABILITIES

UNPRECEDENTED VISIBILITY ACROSS USB DEVICE USAGE — EFFORTLESSLY

Discover devices automatically
Gain continuous insight into USB devices across your organization, including those not covered by a policy. Falcon Device Control automatically reports device type (e.g. mass storage, human interface, etc.) with manufacturer, product name, and serial number. You have visibility into all devices operating over the USB bus, including internal/non-removable USB devices and those not categorized as USB by Windows, such as Bluetooth.

A wealth of information at your fingertips
Immediately see which devices are used in your environment and how they are being used at a glance via usage dashboards. Falcon Device Control provides insight into specific files copied to a removable drive, processes executed from USB storage, users, and hosts where USB devices were used.

Immediate and powerful search capabilities
Falcon Device Control provides fast and powerful real-time and historical search capabilities. Examine your environment for vital information such as the devices used on a specific machine and file writes to mass storage.

PRECISE AND GRANULAR POLICY ENFORCEMENT

Strict policy enforcement
Define device control policies for endpoint groups, whitelist and blacklist devices by class, vendor, product serial number and/or specific device ID. Define device control policies for endpoints both on and offline.

See the impact of policies before implementing them
Alerts and dashboards allow you to see how your policies will impact users before rolling them out.

Define granular policies for drives
Allows read/write or read-only access, while blocking execution of applications on USB drives.

Monitor files written to storage
Track data moving from your endpoints to storage, giving you visibility into what's being copied to devices.

Automatically get device information for quick and easy policy creation and management workflows
Falcon Device Control automatically obtains devices' vendor, class model and serial number, without requiring the use of external tools or device managers, allowing you to create policies for all devices being used in your environment.

Allows devices to charge even when access is denied
Charge your USB devices while simultaneously enforcing your device control policies.

SEAMLESS INTEGRATION WITH FALCON ENDPOINT PROTECTION

One agent, one console, one platform
As a 100 percent cloud managed and delivered solution, Falcon Device Control is enabled via the same lightweight Falcon agent, managed by the same console, and fully integrated with the Falcon platform.

Immediate implementation and management
Falcon Device Control hits the ground running and is operational in minutes.

EMPOWERS YOU WITH IMMEDIATE USB DEVICE VISIBILITY AND PROTECTION AT YOUR FINGERTIPS

You want your users to be able to use their portable devices without being exposed to the inherent risks. That's why Falcon Device Control provides the granular visibility and control needed to enable safe device usage, while leveraging the extensibility of the Falcon platform.

UNPARALLELED VISIBILITY AND GRANULAR CONTROL

Falcon Device Control provides unparalleled visibility over USB device usage and granular control over utilization, for fast and easy mitigation of the risks associated with those devices.

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. Falcon seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed hunting. There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches.

CrowdStrike Products

CROWDSTRIKE

OBSERVATIONS FROM THE FRONT LINES OF THREAT HUNTING

A 2018 Mid-Year Review From Falcon OverWatch

003551

INTRODUCTION

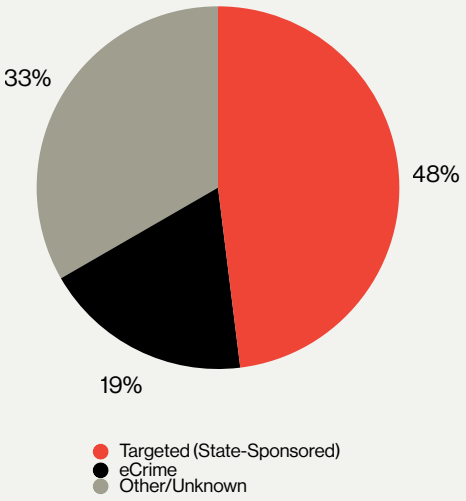
CrowdStrike® Falcon® OverWatch™ is the CrowdStrike managed threat hunting service (MDR). OverWatch's mission includes using the market-leading CrowdStrike Falcon endpoint security platform to detect intrusions by sophisticated or persistent adversaries that might otherwise go unnoticed, and then providing timely, actionable and relevant notifications to customers [1].

This report provides a summary of OverWatch's findings from intrusion hunting during the first half (January through June) of 2018. It reviews intrusion trends during that time frame, provides insights into the current landscape of adversary tactics and delivers highlights of notable intrusions OverWatch identified. OverWatch specifically hunts for targeted adversaries. Therefore, this report's findings cover state-sponsored and targeted eCrime intrusion activity, not all forms of attacks.

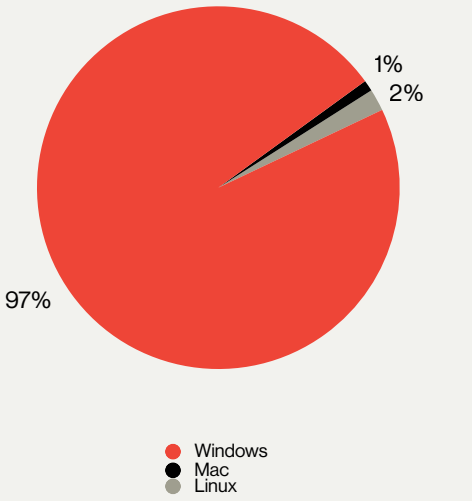
INTRUSIONS SUMMARY

OverWatch observed and analyzed numerous intrusion events during this time period.

INTRUSION CASES* BY THREAT TYPE



INTRUSION CASES* BY OPERATING SYSTEM



*Percentages in these graphs reflect only those intrusion cases involving notable sophisticated and/or persistent adversaries.

[1] For more information on how Falcon OverWatch performs its mission, please see the Falcon OverWatch product page: https://www.crowdstrike.com/products/falcon-overwatch/

PERCENTAGE OF INTRUSION CASES BY VERTICAL

Note: Combined percentages add up to more than 100% because some victims belong to more than one vertical.

While OverWatch analyzed numerous intrusions during this period, only some could be attributed to an adversary at this time. CrowdStrike Falcon Intelligence™ has tracked over 110 specific adversary groups, as well as many unidentified actors. The following chart shows the number of intrusion cases attributed to an adversary by industry vertical.

Vertical	VENOMOUS BEAR	Suspected BEAR	AURORA PANDA	JUDGEMENT PANDA	LOTUS PANDA	PIRATE PANDA	WICKED PANDA	Suspected PANDA	HELIX KITTEN	OCEAN BUFFALO	CARBON SPIDER	Suspected SPIDER
Academic												3
Agriculture												1
Biotechnology				1								
Defense								5				
Energy					1							
Entertainment								1				
Financial	2											
Food & Beverage											1	1
Hospitality						1				1		4
Insurance												2
Internet Services							2					
Legal												1
Mining							2					
NGO		1						5				
Pharmaceutical				1					2			
Professional Services		2					2	5				
Retail											2	2
Technology		1	1				2	9				1
Telecommuni-cations								1				2
Think Tanks		1										
Transportation & Logistics								1				1

When the Falcon OverWatch team analyzes an intrusion, it uses the MITRE ATT&CK™ matrix[2] as a framework to categorize adversary behavior. A heat map of observable tactics, techniques and procedures (TTPs) that were tracked across sophisticated and/or persistent intrusions through the first half of 2018 is available in the Appendix at the end of this report.

[2] More information about Mitre's ATT&CK matrix is available online at: https://attack.mitre.org/wiki/ATT%26CK_Matrix

E-CRIME ACTORS SHOW INCREASING INTEREST IN CRYPTOCURRENCY MINING

During the first quarter of 2018, Falcon OverWatch identified multiple intrusions against victims in the legal and insurance industries where criminal perpetrators gained privileged access to internal networks. Historically, the OverWatch team has seen such actors take advantage of their access to steal sensitive information that could be used for financial gain. However, in these cases, adversaries pursued post-exploitation financial gain by deploying cryptocurrency miners. They employed techniques that allowed them to perform extensive lateral movement, creating as large a foothold as they could to commandeer mining resources. It appears that the rise in the value of cryptocurrencies during the winter of 2017 led eCrime actors to shift their preferred objectives in several cases. Two examples of these intrusions are the following:

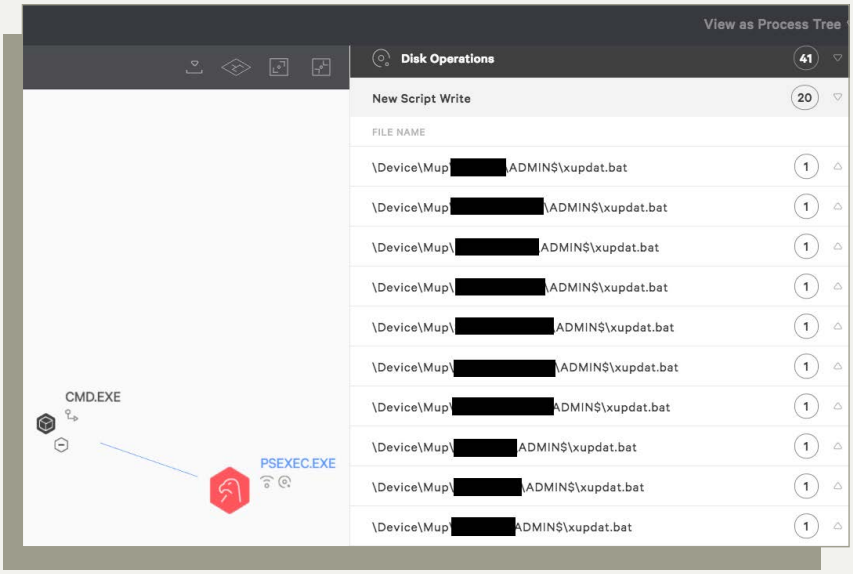
- In January, OverWatch observed an unidentified criminal actor installing a number of malicious tools on compromised hosts belonging to an organization in the legal vertical. These tools included the xDedic[3] RDPPatch tool, the Monero cryptocurrency mining tool XMRig and a disk usage tool used for reconnaissance purposes.
  - RDPPatch allows threat actors to patch the Windows RDP substitution system, which then supports multiple user logins to the compromised host. The RDPPatch binary used in the attack was:
    FILE: C:\Temp\3\Temp1_xrdp.zip\xRdp.v2.1.exe
    HASH: daddc833bffcade36b432b21046487b29dcd2a162d91b503334a52caee9c1fd2
  - XMRig is an open-source Monero cryptocurrency mining software distributed via a public code repository. During this intrusion, the actor attempted to download and install XMRig with the likely intent to passively generate revenue while the host was not otherwise in use:
    FILE: XMRig 64bit version 2.4.3
    HASH: 08b55f9b7dafc53dfc43f7f70cdd7048d231767745b76dc4474370fb323d7ae7
    NOTE: Installed from minergate[.]com/download/win-srv
  - The disk usage tool observed was the otherwise legitimate tool, TreeSize[4]. TreeSize provides an operator with the ability to easily view disk space usage, which could facilitate actions on objectives.
- In late January, Falcon OverWatch assisted CrowdStrike Services in responding to an engagement on the network of an organization in the insurance vertical. OverWatch uncovered widespread malicious activity involving WMI and PowerShell on multiple hosts. Among the extensive telemetry collected during the intrusion were several notable TTPs, including:
  - Attempts to download Pupy RAT[5] files from **https://54.183.214[.]137:8080/eiloShaegae1** and **https://54.183.214[.]137:8080/IMo8oosieVai**
  - Accessing the Domain Controller via RDP using valid credentials
  - Use of PowerShell for host reconnaissance and credential theft
  - Creation of malicious scheduled tasks via Microsoft Management Console

Beyond these behaviors, the adversary also used PsExec to execute a batch file on numerous hosts.

[3] xDedic is a criminal Russian underground marketplace that brings together affiliates who want to either buy or sell access to compromised dedicated RDP servers. The compromised servers are used for activities such as spam email or as VPN endpoints.

[4] https://www.jam-software.com/treesize_free/

[5] https://github.com/n1nj4sec/pupy



Adversary use of PsExec to deploy xpudate.bat to various hosts in an attempt to install Monero miners across the victim network.

The batch script, named xupdate.bat, used PowerShell to download and install a Monero miner:
FILE: C:\Program Files\MSUtil\x.exe
HASH: 85623bf5df6e1ad047bc1b8e94e1db91b922907357251cb7451e1507a38c6426
NOTE: Downloaded from https://bread.rumpus[.]press/zwxjwy

The rise in the value of cryptocurrencies during the winter of 2017 led eCrime actors to shift their preferred objectives in several cases.

BLURRED LINES CONTINUE

A key theme noted in the CrowdStrike 2018 Global Threat Report was the blurring of lines between the TTPs of highly skilled nation-state adversaries and their criminally motivated counterparts. That trend has continued as CrowdStrike saw less skilled criminal actors adopt more advanced TTPs used by well known nation-state actors. One specific manner in which this recurring trend was observed was with the malicious use of TeamViewer software. TeamViewer is a legitimate, publicly available remote control software tool[6]. Malicious use of TeamViewer came to light in 2013 when the adversary that CrowdStrike first tracked as TEAM BEAR was found using the software maliciously to facilitate remote access to targets. Malicious versions of TeamViewer ensured persistence on victim machines, hid their locations and were configured to report to command and control (C2) servers. Since 2013 when TEAM BEAR's tactics were publicly reported, multiple adversaries possessing varying levels of capability and intent, including criminal, have adopted the malicious use of TeamViewer in their operations. Despite extensive public exposure of this known threat, even recently[7], OverWatch continues to see the malicious use of TeamViewer plague organizations across the spectrum of industry verticals.

[6] https://github.com/n1nj4sec/pupy

[7] https://blog.avast.com/update-ccleaner-attackers-entered-via-teamviewer

- In the first quarter of 2018, OverWatch uncovered malicious activity leveraging TeamViewer specifically targeting the hospitality sector. At the time of this writing, at least four global hospitality organizations were victimized during the quarter. In each case, TeamViewer binaries were masquerading as otherwise expected file names, including **msoobe.exe** (Microsoft Out-of-Box Experience) and **jusched.exe** (Java Update Scheduler). Victims' TeamViewer config files had also been modified so that TeamViewer network communications would connect to actor-controlled C2 nodes.

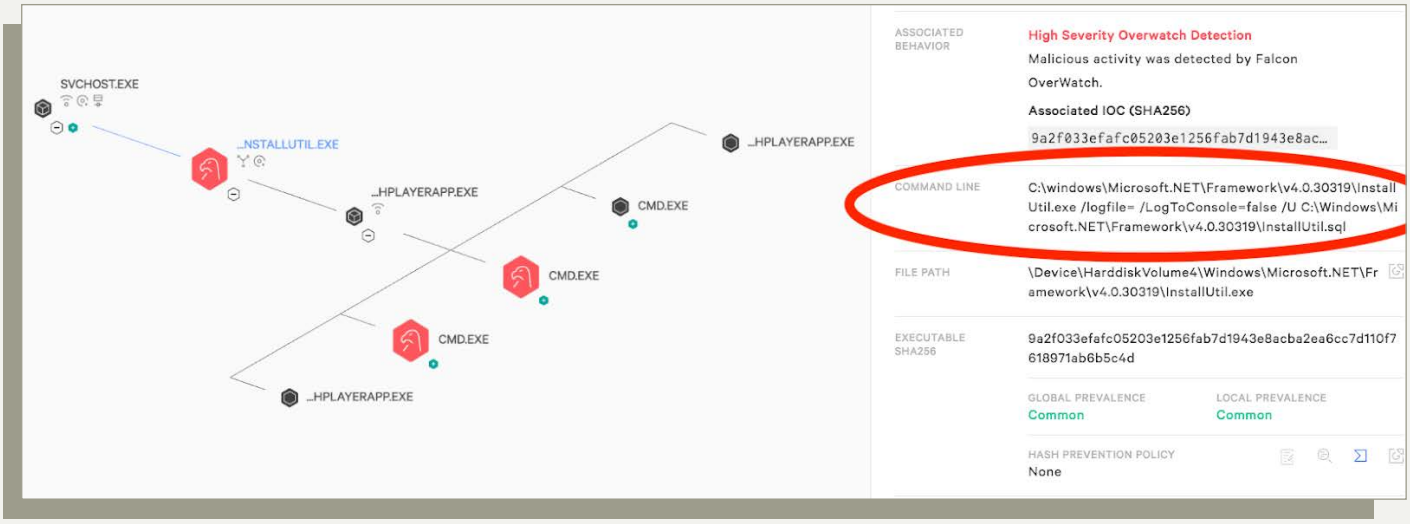
  The malicious TeamViewer activity at each hospitality victim shared overlapping C2 infrastructure, indicating a common adversary was responsible. C2 domains observed in this campaign were:

  - **teravisore[.]ru**
  - **votonafo[.]ru**
  - **sistemappruve[.]ru**
  - **lirubhdk1753[.]ru**

- In January, an unknown actor gained remote access to the network of an entertainment organization. Among the behaviors observed were WebDAV scans, enumerating SMB shares, lateral movement and creating malicious scheduled tasks via schtasks.exe and at.exe. The initial entry, however, was via TeamViewer. The adversary used valid credentials to log into TeamViewer remotely, and then dropped various malicious tools that facilitated the extensive follow-on activity.

Despite extensive public exposure of this known threat, even recently, OverWatch continues to see the malicious use of TeamViewer plague organizations across the spectrum of industry verticals.

After gaining initial access to the network via TeamViewer, the actors moved laterally to another host and deployed PlugX using a method that leverages InstallUtil.exe[8] to bypass whitelisting. InstallUtil.exe is a Microsoft signed binary that can run any .NET executables, bypassing AppLocker restrictions while doing so. OverWatch has observed actors exploiting that capability by recompiling malicious payloads as .NET executables and running them with InstallUtil. The command line in the Falcon console detection of this event demonstrates the tactic:



Adversary use of InstallUtil.exe to deploy PlugX implant.

As noted in the image above, InstallUtil.exe executes with a command line employing the following format:
InstallUtil.exe "/logfile= /LogToConsole=false /u" {path to implant}

In this case, the path to the implant points to a previously unknown InstallUtil.sql file. This binary was dropped by the adversary and further analysis identified it as a variant of the PlugX RAT, which is malware commonly associated with PANDA threat actors. PlugX has been designed to leverage Dynamic-Link Library (DLL) side-loading[9] to successfully obtain execution, typically via a legitimate and signed host binary. During this event, PlugX was side-loaded by the otherwise legitimate FlashPlayerApp.exe process spawned by IntallUtil.exe as shown in the process tree above. The adversary then was able to leverage PlugX to initiate the the interactive cmd.exe shells.

IT CAN HAPPEN TO ANYONE

In March, a business technology solutions organization began deploying the Falcon platform across its network. OverWatch quickly identified evidence of an ongoing, legacy intrusion. An adversary was actively targeting the web-hosting branch of the victim company, resulting in successful exploitation of numerous servers. C2 infrastructure included domains and IP addresses attributed to WICKED PANDA. Malicious network activity in this campaign was seen connecting to the following:

- **backup.aolonline[.]cc**
- **tiwwter[.]net**
- **bot.googlecustomservice[.]com**
- **mall.googlebills[.]net**
- **login.googlebills[.]net**
- **43.239.159[.]41**
- **45.32.9[.]211**
- **103.84.91[.]78**
- **103.84.91[.]146**

During the time of observation, the actor performed limited actions on objectives beyond staging their custom tools, which included PlugX[10]. In this case, OverWatch assesses with moderate confidence that the victim was not the primary target. Rather, the actor was likely taking advantage of this target of opportunity to build their malicious infrastructure to facilitate future operations. An important take-away from this event is the reminder that sophisticated, nation-state adversaries could target anyone as part of a larger operation. OverWatch has observed similar activity across several industry verticals. As a result, customers in any sector could find themselves in the cross-hairs of targeted adversaries.

An important take-away from this event is the reminder that sophisticated, nation-state adversaries could target anyone as part of a larger operation.

[8] https://docs.microsoft.com/en-us/dotnet/framework/tools/installutil-exe-installer-tool

[9] https://attack.mitre.org/wiki/Technique/T1073

[10] https://attack.mitre.org/wiki/Software/S0013

POLICY NGOs A PRIME TARGET

During the last several months, OverWatch has observed multiple adversary campaigns against policy NGOs (nongovernmental organizations) operating overseas. In the first case, threat actors exploited an external server prior to Falcon endpoint protection deployment. Once Falcon was installed, OverWatch was able to identify active use of China Chopper[11] on the victimized server when the adversary connected to the web shell. It appeared the actor had long had a foothold in the environment and was returning to perform access maintenance. Over the course of an hour, they performed host, account and network discovery operations. Specifically, they tested previously compromised credentials by attempting to connect to remote network shares with several valid accounts.

Before leaving, the adversary wrote files associated with the open-source HTran reverse proxy tool[12] in a likely attempt to redirect C2 traffic from additional targets. HTran files were written to the following locations:

- **C:\ProgramData\htran.exe**
- **C:\HR\htran.exe**
- **C:\[REDACTED]\Template\htran.exe**

Falcon endpoint protection customers should be aware that they can turn on Falcon's prevention policy setting to block the Chopper web shell.

A separate and distinct set of adversary activity was also observed against another policy NGO. OverWatch discovered artifacts and active beaconing associated with malicious implants following installation of the Falcon platform across the victim's network. The backdoor of choice in this case was PlugX. As noted before, PlugX remains a prevalent choice for targeted adversaries and historically has been popular among those groups associated with China.

In this case, the legitimate binary used by PlugX for DLL side-loading was a signed BitDefender Crash Handler file:

FILE: C:\ProgramData\DSSM\log.exe
HASH: 386eb7aa33c76ce671d6685f79512597f1fab28ea46c8ec7d89e58340081e2bd

Once running, the malicious process was observed making network connections to the following nodes:

- **46.101.119[.]159:80**
- **46.101.119[.]159:443**

No further actions on objections were observed. While both of these campaigns against policy NGOs involve tactics bearing hallmarks of previously observed Chinese targeted intrusions, CrowdStrike has not yet attributed this activity to a specific adversary.

[11] https://attack.mitre.org/wiki/Software/S0020

[12] https://github.com/zcnhonkerHTran

FURTHER TARGETING OF THE BIOTECHNOLOGY INDUSTRY

OverWatch has observed continued targeted adversary interest in the biotechnology industry vertical in recent months. Industrial espionage is the likely motive behind these attacks. During the rollout of the Falcon platform to one such customer in the first quarter of 2018, OverWatch was able to quickly identify an existing breach.

An unknown adversary had established persistence on an infected host belonging to a senior executive in the organization. The Windows Registry had been modified to execute the following PowerShell commands upon execution of Explorer:

- **powershell.exe -noprofile Invoke-Command -scriptblock{$path='C:\Users\[REDACTED]\Application Data\Microsoft\Network\log\inf32.dat';$data=Get-Content $path;foreach($cmd in $data){iex $cmd;}}**

- **powershell.exe -noprofile Invoke-Command -scriptblock{$path='C:\Users\[REDACTED]\Application Data\Microsoft\Network\log\imeins32.dat';$data=Get-Content $path;foreach($cmd in $data){iex $cmd;}}**

These commands leveraged script blocks to read and execute each line in **inf32.dat** and **imeins32.dat**. Analysis of the .dat files revealed them to be keylogger and file extraction utilities, respectively.

In addition to the key logging and file copying performed by the two malicious .dat files, the adversary also connected to the host to actively perform additional exfiltration. Over the course of 44 minutes, the actor employed the compression utility WinRAR (renamed as **winrs**) to create archives of targeted files from within the active user's home Desktop and Documents directories. The files they targeted were very specific to the highly specialized research and intellectual property of the victim company.

Adversary use of WinRAR to prepare specific files of interest for exfiltration.

The archives created were subsequently deleted after exfiltration. As visible in the Falcon UI detection displayed above, the operator used WinRAR's **-ta** flag to select files by a date range. This is a tactic often observed with nation-state or sophisticated adversaries who are maintaining an ongoing collection effort against an organization.

TECHNOLOGY SECTOR INTRUSION EXHIBITS CREATIVE EVASION TECHNIQUES

In March, a persistent and embedded nation-state adversary returned to a victim network in the technology sector to perform further intrusion operations. The actors gained access via RDP by leveraging valid credentials. They then demonstrated defensive evasion creativity by using the legitimate Microsoft certutil.exe and expand.exe tools to decode binaries masquerading as Windows Update log files. The decoded files turned out to be the following:

FILE: C:\[REDACTED]\psping.exe
HASH: c8453110682d999223a84146462b0b4fc6979f40a01b60a7b925783b71b2d6ff
NOTE: Legitimate SysInternals PsPing[13] tool

FILE: C:\Users\[REDACTED]\Documents\pie.exe
HASH: b072e3a32aea8ba555614ad573364c8469da7023efec984185168733230a45d0
NOTE: Spetnik TCPing[14] utility

These legitimate scanning tools were executed thousands of times to identify open 3389 ports. Results of their enumeration activity were written to the following file:

FILE: C:\[REDACTED]\a.txt

In the course of scanning wide swaths of internal network IP ranges, the adversary potentially revealed part of their C2 infrastructure by pinging the external IP address **45.77.233[.]19**.

The adversary was intent on covering their tracks beyond disguising the tools they dropped and executed. They also removed numerous entries in the Windows Remote Desktop Connection Client listing within the victim machines' registries. They performed further measures to hide evidence of their presence by clearing a wide array of log files using wevtutil.exe. A summary of the defense evasion techniques employed by this committed adversary is provided in the following table:

Defense Evasion Technique(s)	Specific Activity Observed	Commands Observed
Masquerading and Deobfuscate/Decode Files or Information	Used certutil.exe and expand .exe tools to decode malicious binaries masquerading as Windows Update log files	**certutil.exe -decode KB285032.log KB273171.log** **expand KB273171.log pie.exe**
Indicator Removal on Host	Cleared RDP connections history	**reg delete "HKCU\Software\ Microsoft\Terminal Server Client\Default" /va /f** **reg delete "HKCU\Software\ Microsoft\Terminal Server Client\Servers" /va /f**
Indicator Removal on Host	Viewed and cleared event logs	**wevtutil el** **wevtutil cl "Application"**

[13] https://docs.microsoft.com/en-us/sysinternals/downloads/psping

[14] https://tcping.soft32.com/

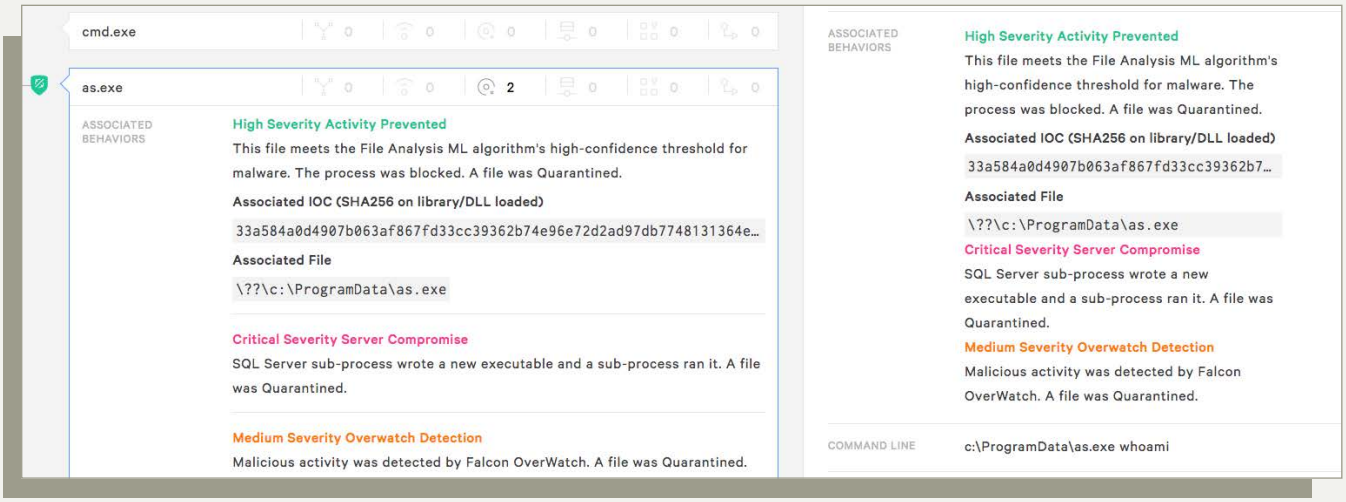
CROWDSTRIKE FALCON STOPS ANOTHER BREACH IN ITS TRACKS

A recent intrusion against the hospitality sector again proved the effectiveness of the Falcon platform in stopping breaches. The victim organization had an externally facing SQL server that was unknowingly exploited prior to the victim moving it to the internal network. After the customer placed it inside their DMZ and installed the Falcon sensor on it, OverWatch was able to identify the intrusion. An unknown, likely criminal adversary was observed returning to the victimized server to perform access maintenance.

The actors initially performed taskkill.exe commands in attempts to kill an array of potentially existing security products. However, their attempts to disable Falcon were unsuccessful. (Current versions of Falcon for Windows and Mac include the ability for an organization to set additional safeguards that will help to prevent the sensor from being uninstalled even by users with administrative privileges.) In conjunction with the taskkill.exe commands, the operators also ran cacls.exe to determine permissions for disabling the security tools.

Later, the adversary attempted to deploy a large number of tools to further build on their beachhead within the network. However, Falcon blocked their attempted expansion and exposed their use of external IP address **222.186.58[.]186** for C2.

Among the tools they attempted to use was a privilege escalation tool[15] that exploits CVE-2016-0099 (MS16-032):
FILE: C:\ProgramData\as.exe
HASH: 33a584a0d4907b063af867fd33cc39362b74e96e72d2ad97db7748131364eab1



CrowdStrike Falcon endpoint protection blocking execution of privilege escalation tool.

Other tools the operator attempted to employ included:

- **Cryptocurrency miner**
- **SQLCrack**[16]
- **Packed version of SysInternals PsKill**[17]
- **TCP scan utility**
- **iSQL query tool**

Thanks to Falcon, the impact of this pre-existing intrusion was mitigated and the attackers were finally thwarted.

[15] https://github.com/zcgonvh/MS16-032/blob/master/ms16-032/ms16-032.cpp

[16] https://www.nccgroup.trust/uk/our-services/cyber-security/products-and-cloud-services/information-security-software/

[17] https://docs.microsoft.com/en-us/sysinternals/downloads/psping

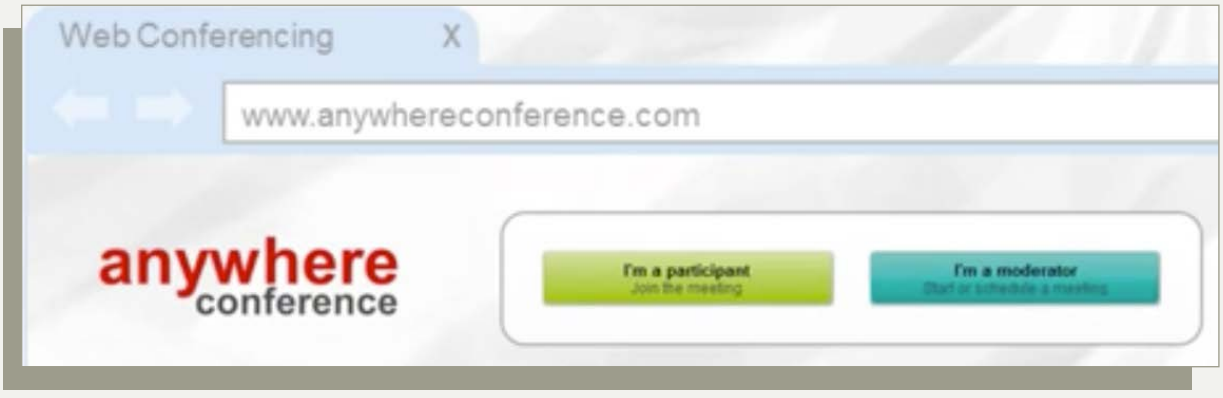
ADVERSARY ATTACKS THINK TANK WITH COMPROMISED TELECONFERENCING SOFTWARE

In April 2018, Falcon OverWatch detected targeted activity on the network of a think tank organization utilizing a set of relatively rare TTPs. The attack began when a user received a spear-phishing message. The sender, claiming to be a university professor hosting a series of webinars for students, asked the targeted victim to join one of the webinars as an expert in the class topic of global politics and economics. The victim user proceeded to follow the sender's instructions to install a teleconferencing application in order to join the webinar. Unbeknownst to the victim, the teleconferencing application was actually a trojanized version of the legitimate Arcadin Vision Desktop App program. As part of the installation, the victim downloaded and extracted the following malicious files:

FILE: C:\Users\[REDACTED]\AppData\Local\Temp\Temp1_VisionDesktopApp.zip\VisionDesktopApp.exe
HASH: 9cbcfb735db96abf9b0774f5311a69bd8bec45beaddae8adb38cae085275d3e6

FILE: C:\Users\[REDACTED]\AppData\Local\VisionDesktopApp\VisionDesktopApp.exe
HASH: c76fbf957b158aa78239e3a3bd8f478fe7a35f1237c6f730b57b6b318fc9ddad

During subsequent installation, these binaries fetched and executed second stage payloads from the adversary's C2 domain anywhereconferencelic[.]com, which the attacker had created to spoof the legitimate domain of Arcadin's teleconferencing service "Anywhere Conference."



Snapshot of the legitimate "Anywhere Conference" website, spoofed in this attack as anywhereconferencelic[.]com to disguise malicious C2 communications.

Following the C2 connections, the actors performed hands-on-keyboard activity. Initially, they carried out brief host reconnaissance, enumerating the local user account and network interfaces. They returned shortly thereafter to drop additional second stage tools, including the following implant:

FILE: C:\Users\[REDACTED]\AppData\Roaming\aylnlfdx.exe
HASH: 1c02630c75d85a3ae59de0a22d3bb82411957ad2cb93626d54f48138c9b0e9e2
C2 : 89.34.111[.]113

The adversary then attempted to establish persistence via a scheduled task by executing the following command:

schtasks.exe /Create /Sc MINUTE /MO 2 /TN "Microsoft Windows DataBase Components" /TR "C:\Windows\TEMP\wdusrv.exe

Minutes later, OverWatch identified the use of a Meterpreter reverse shell attempting to run Mimikatz, but the operation was blocked by the Falcon sensor. The attacker then downloaded an OpenSSL certificate, presumably to secure C2 communications. During this phase, C2 traffic to **asbisua[.]com** was identified, which represents another possible attempt to hide the malicious nature of this activity because the domain closely resembles the website for the legitimate Ukraine-based communications technology distributor, ASBIS. Another defense evasion technique OverWatch uncovered was the actor's use of the Windows "extract" command to uncompress a malicious .dat file containing malicious files, followed by use of the "attrib" command to manipulate the visibility of those files.

The host targeted in this intrusion belonged to an employee of the think tank who was responsible for event coordination. While there is no evidence to confirm that the affected host was specifically targeted by the actor, OverWatch has observed targeted intrusion adversaries focusing on personnel involved in event coordination for think tank organizations in the past. These individuals are of interest to nation-state actors because they may possess information that could facilitate targeting of events involving key individuals involved in global affairs.

This campaign bears similarities to another that also used a fake university professor persona to facilitate targeting of bitcoin exchanges[18]. Social engineering tactics were used to convince victims to install fake GoToMeeting software. If the victim proceeded to join a staged call, the attackers would claim technical difficulties while carrying out actions on objectives.

EXTENSIVE DEFENSE EVASION TECHNIQUES OBSERVED IN INTRUSION AGAINST A UNIVERSITY NETWORK

The Falcon OverWatch team often sees attempts to breach universities, likely due to the potentially valuable research, financial and personal data resources available on those networks. Academic institutions also have reputations for somewhat relaxed IT security postures, providing adversaries with potential opportunities to easily build malicious network infrastructures to facilitate additional attacks elsewhere.

During Q2, OverWatch observed an unknown adversary conducting operations against American universities. In one case, the attacker employed smbexec[19], an open source tool that leverages Samba tools, to provide a PsExec-style shell. Under smbexec, the operator created a new user account, "SQLDebugger," and added it to the local administrators group. They also performed reconnaissance and deployed additional tools to dump credentials, including the following binary:

FILE: C:\Users\SQLDebugger\Desktop\gp2.exe
HASH: 25f236981c13620575967d4e0521539920c6b8eb9140f0fc15d000a36ed157e8

NOTE: This file was also seen with a filename of 'IODPS.exe' in a similar attack at another university.

[18] https://www.slideshare.net/JISC/parallel-session-security

[19] https://github.com/brav0hax/smbexec

After using these dropped tools, the actors immediately overwrote their malicious files with a copy of a legitimate Windows DLL:
copy c:\windows\system32\crypt32.dll gp2.exe /y

They then proceeded to delete their executable files from the filesystem. The actors also deleted the user account they had created (SQLDebugger). These efforts at removing artifacts from the host make recovery and investigation more difficult, and demonstrate a high level of operational security (OPSEC).

About fifteen minutes later, the attackers accessed a second machine using recently stolen credentials. Once again, they employed a remote shell but this time they used a different open-source shell known as CACTUSTORCH[20]. The actors changed shells, possibly, because they were concerned their previous one was detected.

CACTUSTORCH was spawned as a scheduled task in the following manner:
schtasks /create /ru system /sc daily /tr "cmd /c cscript c:\windows\temp\osww.js" /tn osww /f

The adversary then deleted the **osww.js file** from disk, leaving only the copy running in memory via the cscript.exe process. This again demonstrates the remarkable lengths taken to cover their tracks and inhibit response efforts.

The Falcon OverWatch team often sees attempts to breach universities, likely due to the potentially valuable research, financial and personal data resources available on those networks.

WICKED PANDA TARGETS MULTINATIONAL RESOURCES COMPANY

OverWatch identified a targeted intrusion in May 2018 impacting a multinational resources company. The first signs of malicious activity began when a suspicious TeamViewer process on a victim machine wrote the following DLL, which was then loaded into an Explorer process:

FILE: C:\Windows\winmm.dll
HASH: 32998d564425bb796ad55dc464cb0dbf983c1acd200bfd75a8329b7aeed2e2a3

This DLL spoofs a legitimate Windows component of the same name by copying its filename as well as a large number of exported function names. This allows it to be installed on a target system in a location chosen so that it will be loaded by legitimate software via a DLL search-order hijacking technique. When loaded, the DLL acts as a flexible loader for a shellcode payload.

After its installation, the implant connected to the following adversary-controlled infrastructure:

C2 : newspic.x24hr[.]com
C2 : 150.109.37[.]160
NOTE: Registered to Tencent Cloud Computing Co. Ltd., Beijing, China.

The actors used their implant to perform reconnaissance and deploy a number of tools and scripts, including the legitimate "dsquery" tool, likely to perform account and permission groups discovery while attempting to blend in with the native Windows environment. They also dropped the legitimate WinRAR utility and used it to package output from the dsquery tool for exfiltration.

[20] https://github.com/mdsecactivebreach/CACTUSTORCH/blob/master/CACTUSTORCH.js

Another malicious file installed during this phase of the attack was the following implant:

FILE: C:\ProgramData\DatacardService\version.dll
HASH: 54cb25a1d7c71e01920929e834b9376e50636a83ac12f2135730e59c56de72df
C2 : newspic.x24hr[.]com

In addition, the adversary installed the following legitimate service file, which was then executed as service, and sideloaded the malicious version.dll implant:

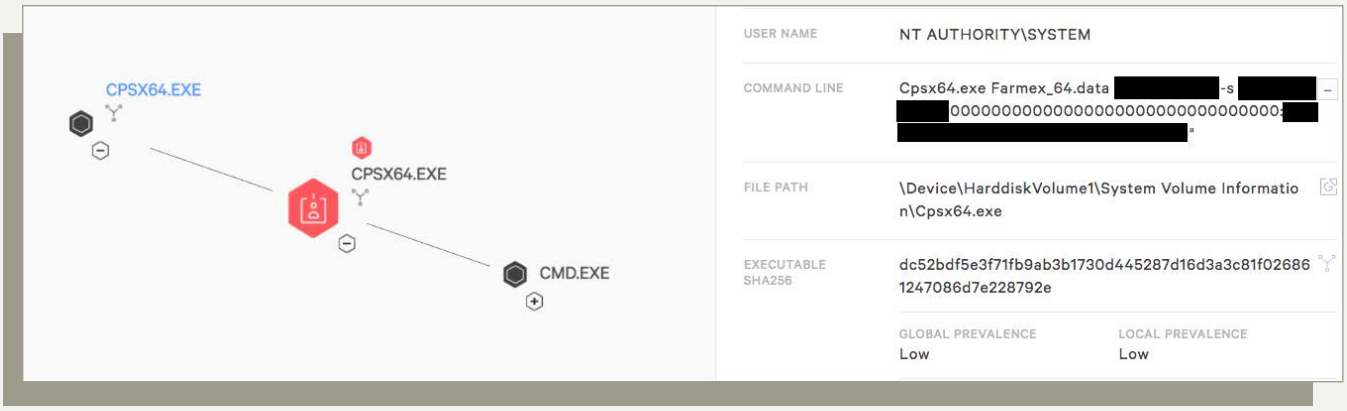
FILE: C:\Users\[REDACTED]\HWDeviceService64.exe
HASH: bb18c63c1982f5cb99c9b65d2b801e8c1909ad7cd0171326dc0015d6b781b451
NOTE: Legitimate service file

Under the newly installed implant, the attacker attempted to dump credentials using a variant of AceHash[21] as well as the Nishang "Get-PassHashes" function[22], but the Falcon endpoint protection platform blocked these operations.

The following day, the actor returned to perform network scanning and then employ the following binary:

FILE: C:\System Volume Information\Cpsx64.exe
HASH: dc52bdf5e3f71fb9ab3b1730d445287d16d3a3c81f026861247086d7e228792e

This tool was executed with the following command line as part of a pass-the-hash attack to facilitate lateral movement to three further hosts in the network, as shown in the Falcon UI here:



Falcon UI display of the pass-the-hash attack

A credential-dumping utility was deployed on the additional victim machines and further reconnaissance was performed. Once the victim organization responded by using the Falcon platform to contain the exploited systems, adversary activity ceased.

Based on the tool, infrastructure, and TTP overlap, CrowdStrike Falcon Intelligence has attributed this activity to WICKED PANDA with medium confidence.

[21] https://jpcertcc.github.io ToolAnalysisResultSheet/details/AceHash.htm

[22] https://github.com/samratashok/nishang/blob/master/Gather/Get-PassHashes.ps1

THREAT ACTOR EMPLOYS SEVERAL CREDENTIAL THEFT TECHNIQUES AGAINST A SINGLE VICTIM

Another intrusion OverWatch analyzed this year involved an unidentified adversary targeting the network of a policy research organization. The attacker gained initial access to a domain controller using valid credentials over an RDP session. The malicious activity included lateral movement attempts to other systems over RDP and SMB shares, as well as reconnaissance of the types of research carried out by various staff.

Throughout the attack, the operator placed a high priority on stealing more credentials, employing several TTPs[23] to do so:

- **Credentials in Files**[24]
- **Credential Dumping**[25]
- **Kerberoasting**[26]

CREDENTIALS IN FILES

The actor employed the "Credentials in Files" technique by using xcopy to gather the domain Group Policy Preference (GPP) files from the domain controller's SYSVOL folder with the following command:

```
xcopy /S /E /C /Q /H \\[REDACTED]\sysvol\[REDACTED]\policies\*.*
```

The purpose of copying GPP files is that they can be mined for credentials and other information, facilitating a deeper foothold in the network.

CREDENTIAL DUMPING

The adversary returned later to perform credential dumping by deploying and executing the legitimate Windows Sysinternals tool "AD Explorer"[27] with the following command:

```
adexplorer -snapshot "" c:\users\[REDACTED]\downloads\adexplorer\\snapshot1.snp
```

This utility provides the ability to save snapshots of the Active Directory database for offline viewing. Later, the actor accessed a SQL server over RDP using valid credentials and deployed the ProcDump utility to dump memory from the LSASS process, providing the attacker with additional credentials.[28] OverWatch also identified that the adversary connected to a third host over a network logon session and attempted to harvest the Ntds.dit file and SYSTEM registry archive from a Volume Shadow Copy. The SYSTEM registry archive contains the key required to decrypt the Ntds.dit file as well as other sensitive information.

KERBEROASTING

The Falcon platform also captured the malicious operator downloading and running the legitimate Windows Setspn[29] tool, which searches for service principal names (SPNs) over the network's domain. This information was used in an attempt to compromise credentials via Kerberoasting. Kerberoasting occurs when an attacker, using a valid Kerberos ticket-granting ticket, requests one or more ticket-granting service tickets for SPNs from the domain controller.

[23] These credential access TTPs are part of the MITRE ATT&CK model, which provides an industry standard for understanding and categorizing adversary post-exploitation behavior. More information available at https://attack.mitre.org/wiki/Main_Page.

[24] https://attack.mitre.org/wiki/Technique/T1081

[25] https://attack.mitre.org/wiki/Technique/T1003

[26] https://attack.mitre.org/wiki/Technique/T1208

[27] https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer

[28] https://docs.microsoft.com/en-us/sysinternals/downloads/procdump

[29] https://technet.microsoft.com/pt-pt/library/cc773257(v=ws.10).aspx

These tickets may be vulnerable to offline brute force attacks that can expose plaintext credentials. In this case, OverWatch identified the adversary retrieving and executing a PowerShell script that employed PowerSploit's Invoke-Kerberoast module, which requests service tickets and returns crackable ticket hashes.

While the Falcon OverWatch team commonly sees attempts to harvest credentials during targeted intrusions, this case was unique in the number of techniques observed. The attackers clearly placed credential theft as a top priority for their operation, likely with the intention of maintaining access to a network they consider a high-value target.

CONCLUSION

During the first half of 2018, Falcon OverWatch continued to identify and analyze a growing number of sophisticated and/or persistent intrusions. The technology, professional services and hospitality sectors were targeted most often, but government-sponsored and criminal adversaries attacked victims across a wide range of industries. The actors used a variety of techniques, demonstrating particular creativity and perseverance in defense-evasion and credential-access TTPs. OverWatch sees no evidence suggesting these trends will EDR change significantly over the next several months.

Threat hunting across detailed endpoint data, such as that collected by EDR (endpoint detection and response) tools like CrowdStrike Falcon, is invaluable in identifying stealthy adversaries using these types of TTPs and evasions. All organizations that are at risk from these threats should deploy threat hunting teams — internal or MDR services like Falcon OverWatch — to rapidly detect, investigate and remediate intrusions before adversaries can accomplish their objective and cause a data breach.

One of the key metrics that CrowdStrike OverWatch tracks for all intrusions it identifies is breakout time, the time it takes for an intruder to begin moving laterally outside of the initial beachhead to other systems in the network. The current average breakout time is 1 hour and 58 minutes, which means that if defenders are able to detect, investigate and remediate the intrusion within 2 hours, they can stop the adversary before they can cause serious damage. CrowdStrike recommends that all organizations adopt the "1-10-60" rule:

- **Strive to detect a threat in 1 minute on average**
- **Investigate the detection in 10 minutes**
- **Remediate and contain the attack in 1 hour**

APPENDIX

CROWDSTRIKE FALCON OVERWATCH INTRUSIONS MAPPED TO MITRE ATT&CK FRAMEWORK (H1 2018)

INITIAL ACCESS 10 items	EXECUTION 31 items	PERSISTENCE 56 items	PRIVILEGE ESCALATION 28 items	DEFENSE EVASION 59 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CMSTP
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Code Signing
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Component Firmware
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Component Object Model Hijacking
Valid Accounts	Install	Change Default File Association	Extra Window Memory Injection	Control Panel Items
	InstallUtil	Component Firmware	File System Permissions Weakness	DCShadow
	Local Job Scheduling	Component Object Model Hijacking	Hooking	Deobfuscate/Decode Files or Information
	LSASS Driver	Create Account	Image File Execution Options Injection	Disabling Security Tools
	Mshta	DLL Search Order Hijacking	Launch Daemon	DLL Search Order Hijacking
	PowerShell	Dylib Hijacking	New Service	DLL Side-Loading
	Regsvcs/Regasm	External Remote Services	Path Interception	Exploitation for Defense Evasion
	Regsvr32	File System Permissions Weakness	Plist Modification	Extra Window Memory Injection
	Rundll32	Hidden Files and Directories	Port Monitors	File Deletion
	Scheduled Task	Hooking	Process Injection	File System Logical Offsets
	Scripting	Hypervisor	Scheduled Task	Gatekeeper Bypass
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Files and Directories
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Users
	Signed Script Proxy Execution	Launch Agent	SID-History Injection	Hidden Window
	SourceSpace after Filename	Launch Daemon	Startup Items	HISTCONTROL
	Third-party Software	Launchctl	Sudo	Image File Execution Options Injection
	Trap	LC_LOAD_DYLIB Addition	Sudo Caching	Indicator Blocking
	Trusted Developer Utilities	Local Job Scheduling	Valid Accounts	Indicator Removal from Tools
	User Execution	Login Item	Web Shell	Indicator Removal on Host
	Windows Management Instrumentation	Logon Scripts		Indirect Command Execution
	Windows Remote Management	LSASS Driver		Install Root Certificate
		Modify Existing Service		InstallUtil
		Netsh Helper DLL		Launchctl
		New Service		LC_MAIN Hijacking
		Office Application Startup		Masquerading
		Path Interception		Modify Registry
		Plist Modification		Mshta
		Port Knocking		Network Share Connection Removal
		Port Monitors		NTFS File Attributes
		Rc.common		Obfuscated Files or Information
		Re-opened Applications		Plist Modification
		Redundant Access		Port Knocking
		Registry Run Keys / Start Folder		Process Doppelgänging
		Scheduled Task		Process Hollowing
		Screensaver		Process Injection
		Security Support Provider		Redundant Access
		Service Registry Permissions Weakness		Regsvcs/Regasm
		Shortcut Modification		Regsvr32
		SIP and Trust Provider Hijacking		Rootkit
		Startup Items		Rundll32
		System Firmware		Scripting
		Time Providers		Signed Binary Proxy Execution
		Trap		Signed Script Proxy Execution
		Valid Accounts		SIP and Trust Provider Hijacking
		Web Shell		Software Packing
		Windows Management Instrumentation Event Subscription		Space after Filename
		Winlogon Helper DLL		Timestomp
				Trusted Developer Utilities
				Valid Accounts
				Web Service

Number of Intrusions Where Technique Was Observed

1 52

OBSERVATIONS FROM THE FRONT LINES OF THREAT HUNTING

CREDENTIAL ACCESS 20 items	DISCOVERY 19 items	LATERAL MOVEMENT 17 items	COLLECTION 13 items	EXFILTRATION 9 items	COMMAND & CONTROL 21 items
Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Brute Force			Clipboard Data	Data Encrypted	
Credential Dumping	Browser Bookmark Discovery	Distributed Component Object Model	Data from Information Repositories	Data Transfer Size Limits	Connection Proxy
Credentials in Files				Exfiltration Over Alternative Protocol	Custom Command and Control Protocol
Credentials in Registry	File and Directory Discovery	Exploitation of Remote Services	Data from Local System		
Exploitation for Credential Access	Network Service Scanning	Logon Scripts	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Custom Cryptographic Protocol
Forced Authentication	Network Share Discovery	Pass the Hash	Data from Removable Media	Exfiltration Over Other Network Medium	Data Encoding
Hooking	Password Policy Discovery	Pass the Ticket			Data Obfuscation
Input Capture	Peripheral Device Discovery	Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Input Prompt		Remote File Copy	Email Collection		Fallback Channels
Kerberoasting	Permission Groups Discovery	Remote Services	Input Capture	Scheduled Transfer	Multi-Hop Proxy
Keychain		Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
LLMNR/NBT-NS Poisoning	Process Discovery		Screen Capture		Multiband Communication
Network Sniffing	Query Registry	Shared Webroot	Video Capture		Multilayer Encryption
Password Filter DLL	Remote System Discovery	SSH Hijacking			Port Knocking
Private Keys	Security Software Discovery	Taint Shared Content			Remote Access Tools
Replication Through Removable Media		Third-party Software			Remote File Copy
Securityd Memory	System Information Discovery	Windows Admin Shares			Standard Application Layer Protocol
Two-Factor Authentication Interception	System Network Configuration Discovery	Windows Remote Management			Standard Cryptographic Protocol
	System Network Connections Discovery				Standard Non-Application Layer Protocol
	System Owner/User Discovery				Uncommonly Used Port
	System Service Discovery				Web Service
	System Time Discovery				

Number of Intrusions Where Technique Was Observed

1 52

ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint protection. The CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. The lightweight Falcon agent deploys in minutes to deliver actionable intelligence and real-time protection from Day One. The Falcon platform seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by a 24/7 managed hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed. The Falcon platform protects customers against all cyberattack types, using sophisticated signatureless artificial intelligence/machine learning and indicator-of-attack-based (IOA) threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™ database, the Falcon platform instantly correlates over 1 trillion security events per week from across the globe to immediately prevent and detect threats.

Learn more at

www.crowdstrike.com

CROWDSTRIKE

ForeScout

NuHarbor SECURITY

You are invited to the technical hands-on, **Automated Threat Response in Motion** half-day event presented by CrowdStrike, ForeScout Technologies, and NuHarbor Security. This Technical Forum will showcases the latest cybersecurity solutions. You will see and experience how ForeScout CounterACT® 8 and CrowdStrike Falcon® orchestrate information sharing and security workflows to automate your threat response.

ForeScout will highlight:

- **Asset Management.** See how agentless visibility of hardware and software translates into an easy software audit.
- **Device Compliance.** Discover if devices are running up-to-date security software, create a policy that notifies out-of-compliance hosts and confirm that systems are restored to compliance.

CrowdStrike will cover:

- **Hacker Awareness.** Complete advanced attack scenarios — running live malware and executing a phishing and browser based exploit
- **Investigate & Get Visibility.** Discover new methods for dealing with malware, ransomware and spearphishing- get full visibility into each attack step and see how you could stop a breach in your own environment.

Don't miss this unique experience to test drive the products at this exclusive event, and be sure to bring your laptop!

Register

When:

June 28th, 2018

Choose a Session:

Morning: 9:00 a.m. - 1:00 p.m. with lunch

Afternoon: 2:00 p.m. - 6:00 p.m. with happy hour & snacks

Where:

WeWork South Station
745 Atlantic Avenue
7th Floor
Boston, MA 02111

(ISC)2®

CPE Credits Available

(ISC)2 members who attend ForeScout's Automated Threat Response in Motion qualify for up to three continuing professional education credits.

Please provide your (ISC)2 membership number when you register.

Our mailing address is:
190 W. Tasman Dr.
San Jose, CA 95134 USA

Skip to main content

Set Up Single Sign-On (SSO) with Falcon

Version 1.2 - Last updated: 07/26/2018

Contents:

Skip to main content

Introduction

This guide describes how to set up your organization's Falcon console to use single sign-on (SSO) for authentication. This simplifies user management and improves security controls.

If you set up SSO, it replaces Falcon's standard sign-in process. You can temporarily use an "onboarding" mode while you transition between existing Falcon authentication and SSO.

Skip to main content

Before You Begin

Single Sign-On Terminology

You should be familiar with some common, industry-standard terms related to single sign-on.

- **Single sign-on (SSO)**: A single authentication system that can be used to access multiple software systems. You can set up an SSO solution in order to simplify login processes for your users and to centralize user management for your administrators.
- **Service Provider (SP)**: The specific application you want to access via SSO. For this guide, the SP is the Falcon console. Other resources sometimes use the name "relying party (RP)".
- **Identity Provider (IdP)**: The service that handles your SSO authentication and manages your users' identity information. For this guide, the IdP is your SSO solution, such as Okta, Ping, or AD FS.
- **Security Assertion Markup Language (SAML)**: A protocol used to implement SSO. Falcon supports SAML 2.0, a widely used standard that's supported by many IdPs.
- **Application**: A set of configuration options that tells your IdP how to interact with Falcon and that governs which of your IdP users can use SSO to access Falcon.

Supported IdPs

We've tested SSO for Falcon with these IdPs using the Chrome browser:

- Okta
- PingOne
- Active Directory Federation Services (AD FS)

Before continuing, you should have an existing SSO solution that uses one of these IdPs.

Chrome is the only supported browser for accessing the Falcon console.

User Management

- **Creating users**: You must create and activate each user in Falcon before they can log in with SSO. Each Falcon email address must exactly match the information in your IdP.
- **Roles**: Manage Falcon's user roles in Falcon, not in your IdP.
- **Passwords and 2FA**: Reset passwords or configure two-factor authentication (2FA) settings in your IdP, not in Falcon.

Limitations

- Falcon's SSO integration applies only to authentication. In other words, we support identity assertion, including signed and encrypted assertions.
  - Falcon **doesn't** support more complex SSO functionality, such as automatic user account provisioning and de-provisioning, user group management or sync, or single logout.

Skip to main content

1. Configure Your IdP

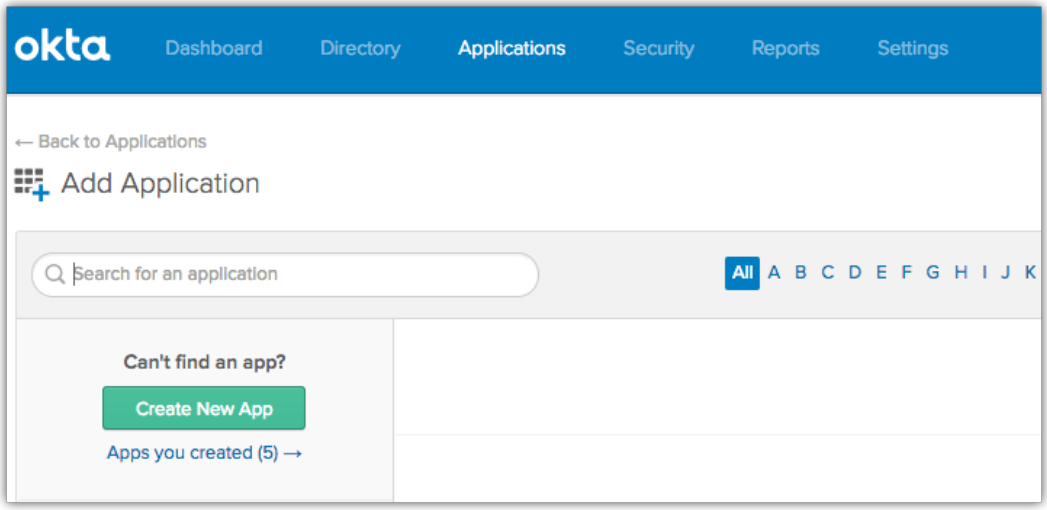
Each IdP has its own process for creating and assigning a new application. The process follows this general pattern:

1. Access your IdP's application settings.
2. Add a new application to your IdP.
   - Provide Falcon's SP URL: `https://falcon.crowdstrike.com/saml/acs`
   - Provide Falcon's SAML metadata: `https://falcon.crowdstrike.com/saml/metadata`
   - Map your users' IdP username to their Falcon email address.
3. Assign your IdP application to your IdP users.

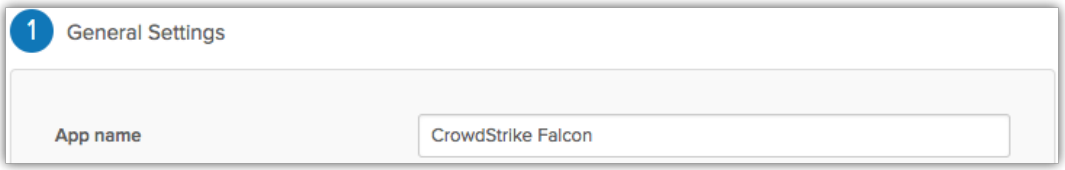
Okta

For more information about configuring Okta, see Okta's documentation.

1. Log in to Okta.
2. Create an application for Falcon.
   1. Go to **Applications**.
   2. Click **Add Application**.
   3. Click **Create New App**.



   4. For **Sign on method**, select **SAML 2.0**.
   5. Click **Create**.
   6. Add required values to your application's configuration:
      - **App name**: a descriptive label, such as "CrowdStrike Falcon"



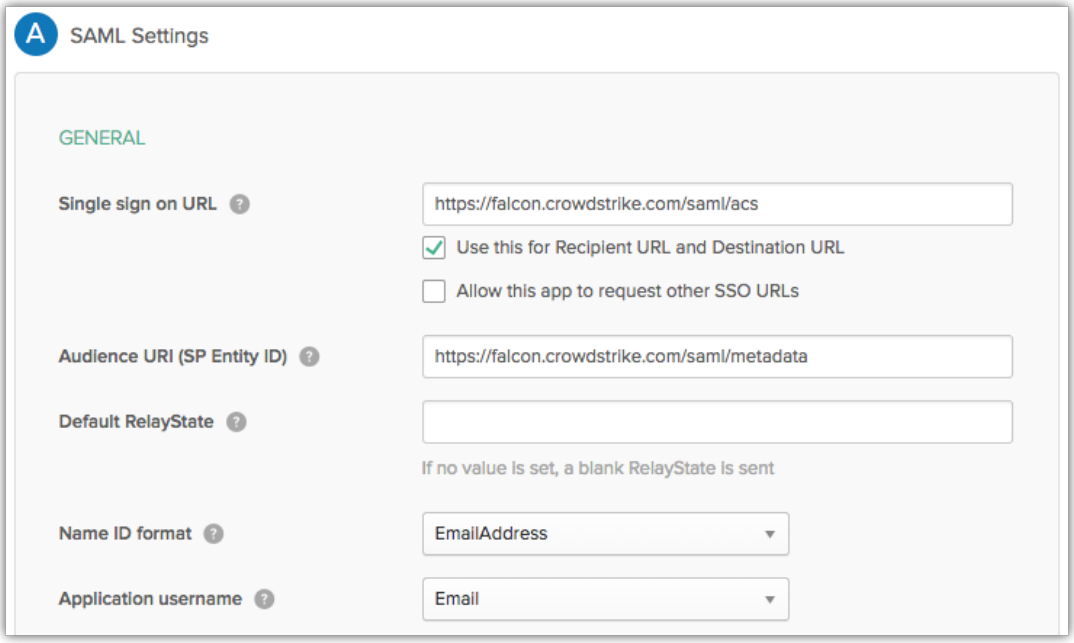
      - **Single sign on URL**: `https://falcon.crowdstrike.com/saml/acs`
      - **Audience URI (SP Entity ID)**: `https://falcon.crowdstrike.com/saml/metadata`

003575

Skip to main content

ame ID format: `EmailAddress`

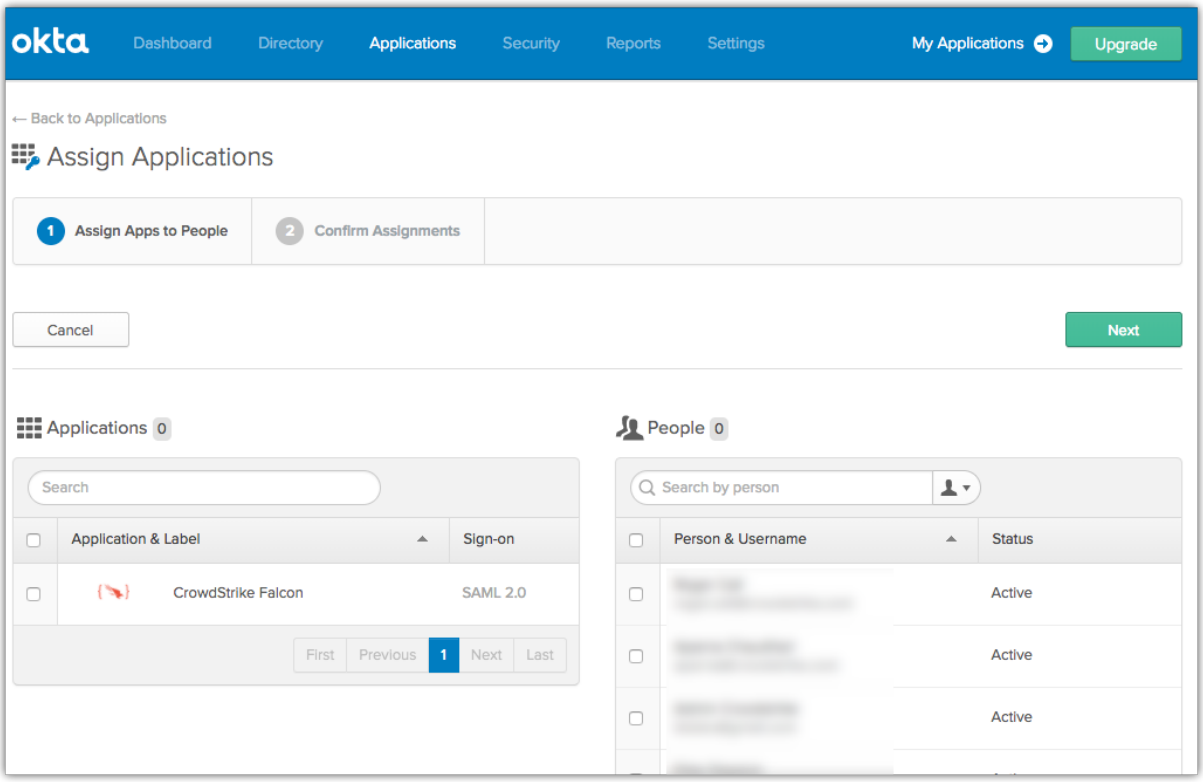
- Application username: `Email`



3. Assign your application to your users.

    1. Go to **Applications**.

    2. Click **Assign Applications**.



    3. Assign your Falcon application to any users you choose.

Tip: When you're first setting up SSO, assign access only to a test user group. You can return later to assign more users throughout your organization.

003576

Skip to main content

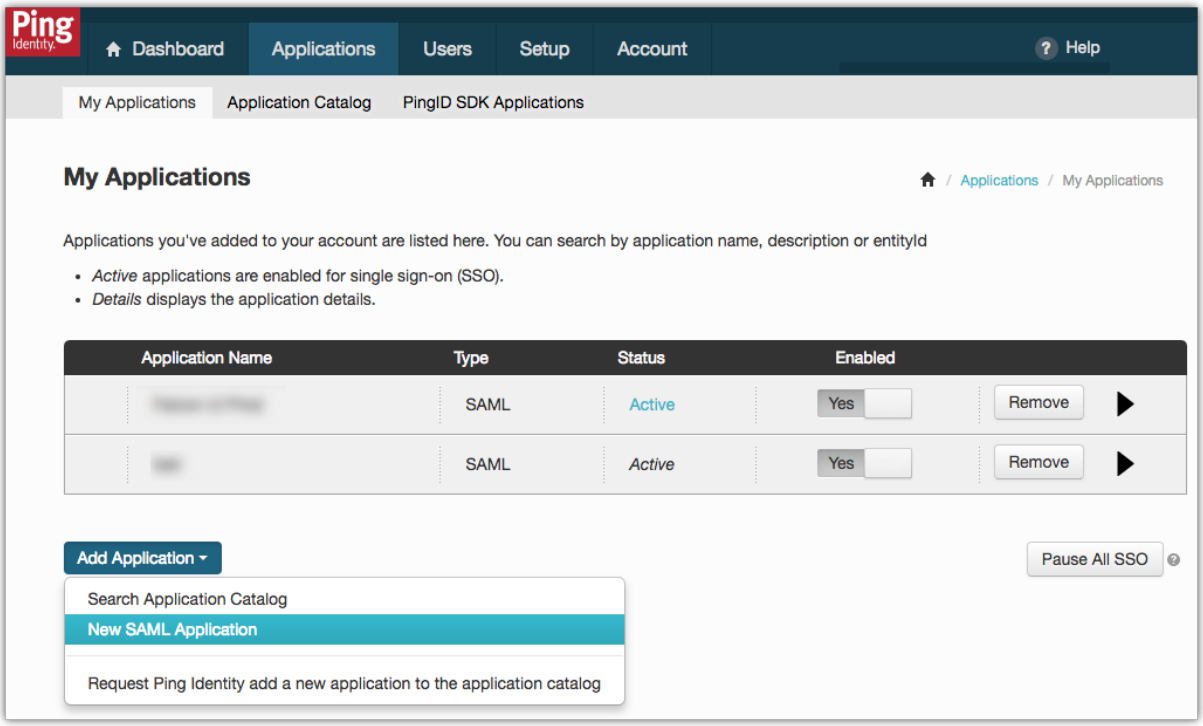
4. Click **Next**.

5. Confirm your users' email addresses.
6. Click **Confirm Assignments**.

PingOne

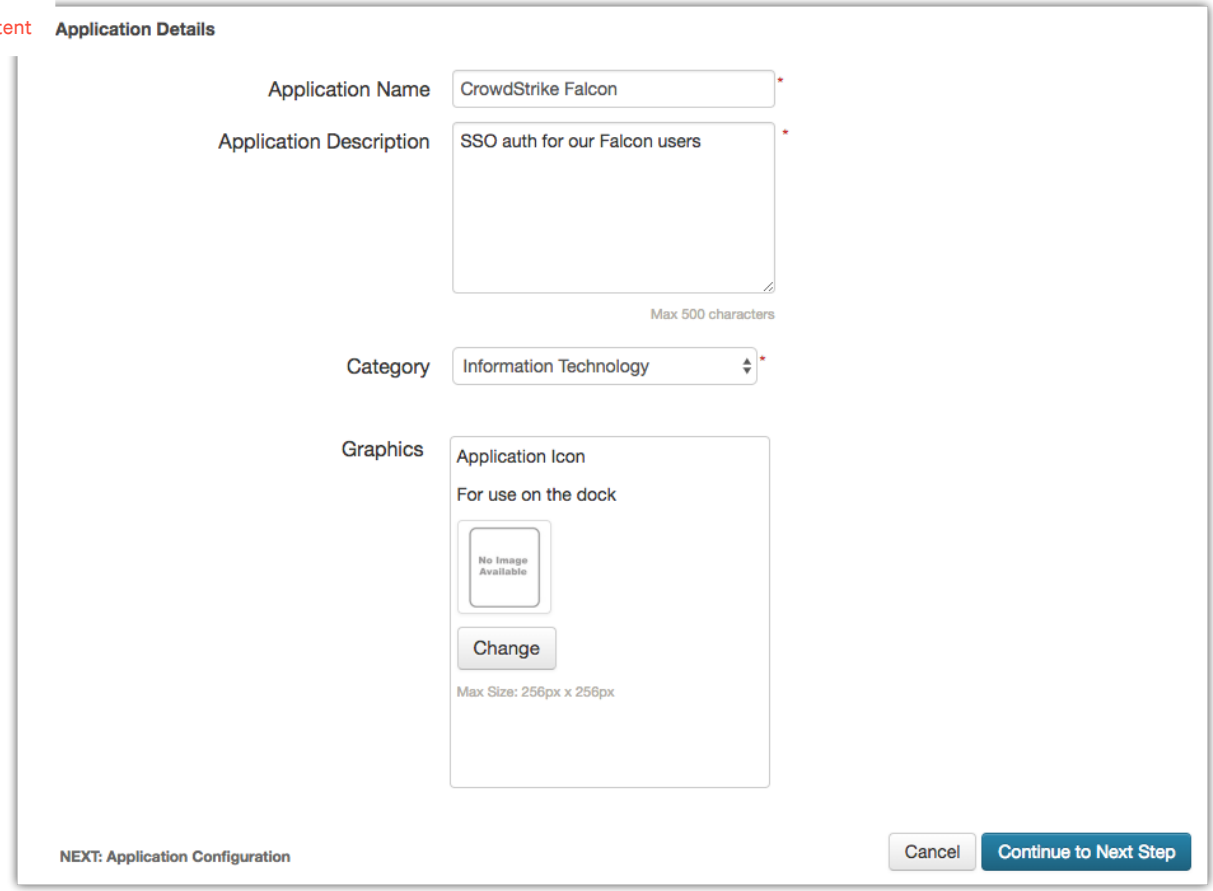
For more information about configuring PingOne, see Ping's documentation.

1. Log in to PingOne.
2. Create an application for Falcon.
    1. Go to **Applications**.
    2. Click **Add Application**.

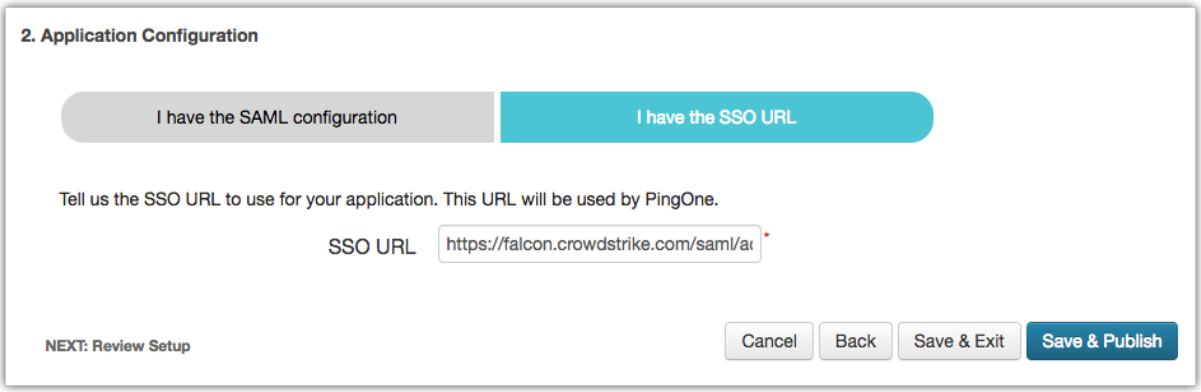


    3. Select **New SAML Application**.
    4. Enter a descriptive label for the required fields:
        - **Application Name**
        - **Application Description**
        - **Category**

Skip to main content



5. Click **Continue to Next Step**.
6. Near the top, select **I have the SSO URL**.



7. For the **SSO URL**, enter: `https://falcon.crowdstrike.com/saml/acs`
8. Click **Save & Publish**.
9. Assign your application to your users.
10. Go to **Users**.
11. Click **User Groups**.
12. Near the group you want to assign access to your application, click **Edit**.

> Tip: When you're first setting up SSO, assign access only to a test user group. You can return later to assign more users throughout your organization.

13. Select your application for Falcon.

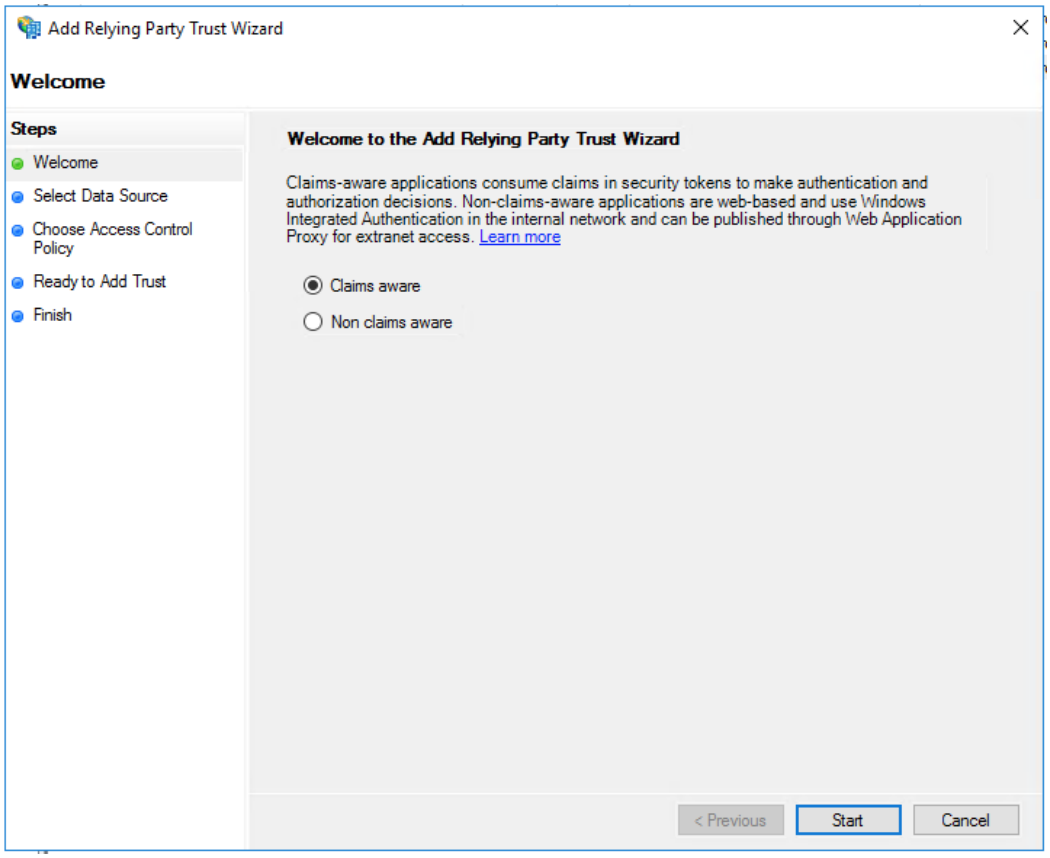
Skip to main content

Save.

Active Directory Federation Services (AD FS)

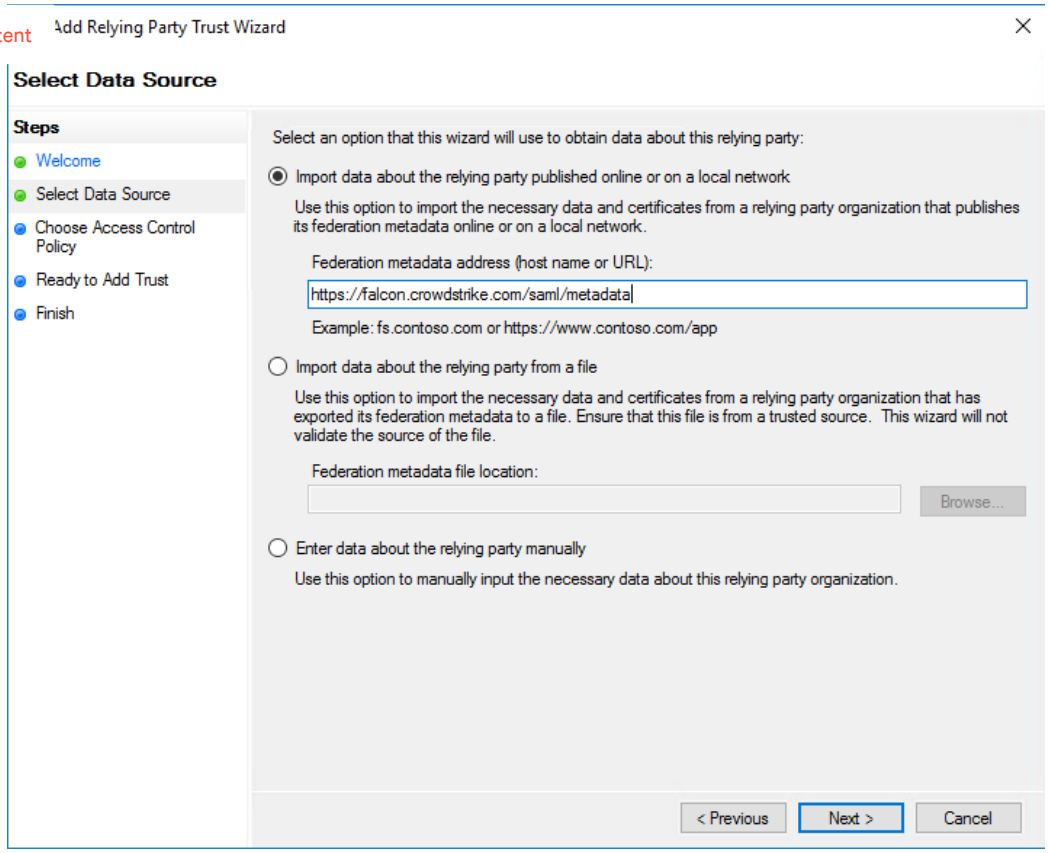
These steps and screenshots shown were taken from AD FS version 4.0 on Windows Server 2016. Similar steps apply to other versions of AD FS or Windows Server. For more information, refer to Microsoft's documentation.

1. Create a new **relying party trust**.
    1. Open your AD FS Management Console.
    2. Add a new **relying party trust**.
    3. Select **Claims aware**.



    4. Click **Start**.
    5. In the **Federation metadata address** field, enter CrowdStrike's metadata URL:

```
https://falcon.crowdstrike.com/saml/metadata
```



If your AD FS server can't access our metadata URL, you can download the metadata XML file from that URL, then use this wizard to import from the file.

6. Click **Next**.

7. Set your trust's name and permissions as required for your AD FS environment.

2. Configure the AD FS claims for your relying party trust to map your users' email addresses to the Name ID field of the SAML response. To do so, create two rules: one for sending claims and one for receiving claims.

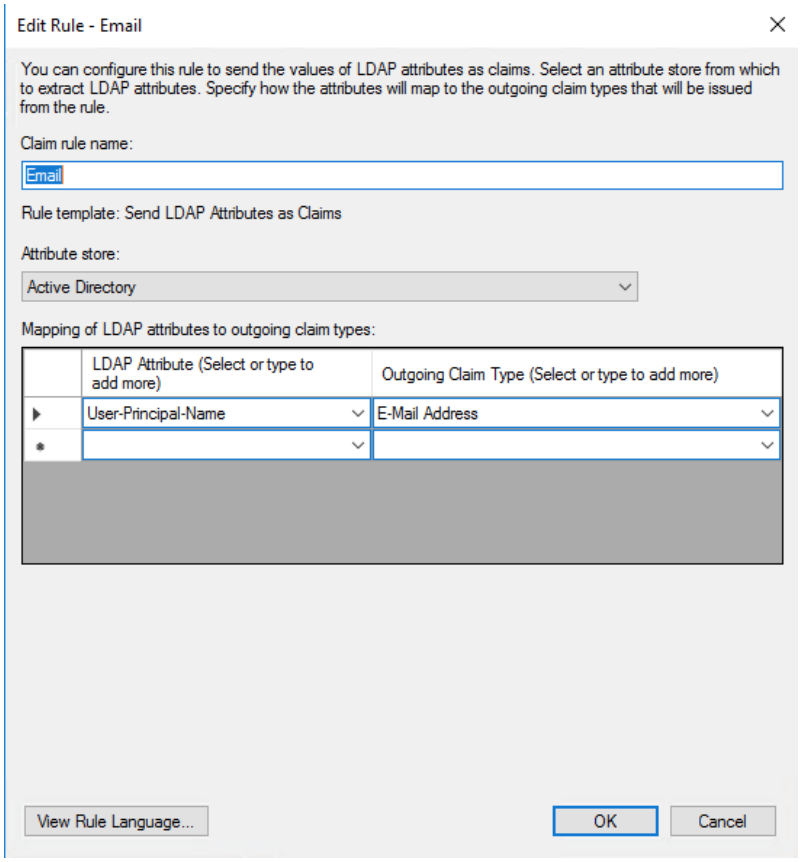
    1. Select your relying party trust, and choose **Edit Claim Issuance Policy**.

    2. Create a rule for sending claims. The specific LDAP attribute varies depending on your AD configuration.

        1. Click **Add Rule**.
        2. For the **Claim rule template**, choose **Send LDAP Attribute as Claims**.
        3. Enter any **Claim rule name** as a descriptive label.
        4. For the **Attribute store**, choose **Active Directory**.

        5. Add one row mapping the LDAP attribute that contains users' email addresses, such as `User-Principal-Name`, to the outgoing claim type `E-Mail Address`.

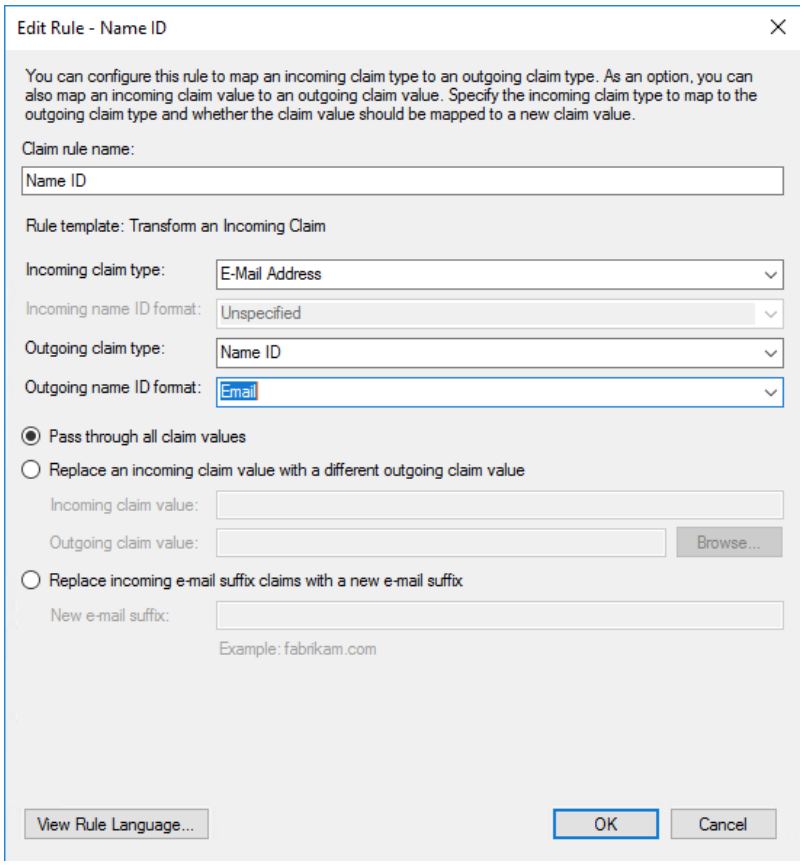
Skip to main content



3. Create a second rule for receiving claims.

    1. Click **Add Rule**.
    2. For the **Claim rule template**, choose **Transform an Incoming Claim**.
    3. Set the following attributes for transforming incoming claims:
        - Incoming claim type: E-Mail Address
        - Outgoing claim type: Name ID
        - Outgoing name ID format: Email
    4. Leave **Pass through all claim values** selected

Skip to main content



RETRIEVING AD FS METADATA

AD FS makes its metadata XML file available at a URL that varies depending on your AD FS configuration (default: `https://<host>:<port>/Federation/Metadata/2007-06/FederationMetadata.xml`).

Falcon only accepts metadata encoded as UTF-8.

Skip to main content

2. Contact Us to Configure Falcon SSO for your Organization

To configure Falcon to communicate with your IdP, contact CrowdStrike support via our support portal. For our support team to complete your SSO request, you must have the role **Falcon Host Administrator** or **Intel Application Admin**.

1. Log in to the support portal.
2. Create a new ticket titled `Request for SSO integration`.
3. Upload your IdP's SAML metadata XML to the ticket. The metadata XML file contains these required attributes:
   - Entity ID (usually in the form of a URL)
   - Redirect URL
   - Public certificate
   - Supported bindings

Our support team receives your ticket and provides you with status updates as needed.

Skip to main content

3. Test Logging In with SSO

After our support team configures your organization to use SSO, we notify you via the support portal. At this point, your Falcon environment is in "onboarding mode."

In onboarding mode, Falcon's login screen accepts your Falcon credentials by default. You can also use a specific URL to log in with your SSO credentials instead. Onboarding mode is intended for temporary use while you test your SSO credentials.

To log in with SSO while in onboarding mode:

1. Open the SSO login URL with the Chrome browser:

   ```
   https://falcon.crowdstrike.com/login/sso
   ```

2. Enter your email address in the **Email** field.
3. Click **Continue**, and the Falcon console redirects you to your IdP's authentication process.
4. Authenticate using your SSO credentials.

> Tip: After you exit onboarding mode, you can log in to Falcon at its usual URL, `https://falcon.crowdstrike.com`, without using the SSO login URL. However, the SSO login URL remains available after you exit onboarding mode.

Skip to main content

4. Transition to SSO Authentication

Once you've successfully tested an SSO user, you're ready to exit "onboarding mode" and authenticate only via SSO.

> **Warning**: After this step, no one in your organization can log in with their Falcon credentials. Be sure that:

- Everyone in your organization understands how to log in via SSO using the Chrome browser
- Your organization's SSO accounts are granted access to the Falcon application in your IdP

To transition to SSO (and disable authentication via Falcon credentials):

1. Log in to the support portal.
2. Create a new ticket titled `Request to exit SSO onboarding mode .`

Our support team receives your ticket and notifies you when the transition to SSO is complete.

When you exit onboarding mode, you can log in either:

- **Through Falcon**: Using the Chrome browser, go to `https://falcon.crowdstrike.com` . When you enter your email address, you're prompted for SSO authentication.
- **Through your IdP**: Using the Chrome browser, log in to your IdP's interface and select your Falcon application.

Skip to main content

Troubleshooting

Issue: Can't Log In with SSO

Check these possible causes in this order:

1. Make sure the user account exists in Falcon.
2. Make sure the user account's SSO username exactly matches their Falcon email address.
3. Make sure the user is provisioned in your IdP to use the application you created for Falcon.
4. Make sure your IdP application uses the correct Falcon metadata XML attributes:
   - Service Provider Entity ID: `https://falcon.crowdstrike.com/saml/metadata`
   - Single Sign-On URL or Security Token Consumer URL: `https://falcon.crowdstrike.com/saml/acs`
   - Name ID Format: the user's email address as shown in Falcon
   - Public Certificate: The certificate information provided at `https://falcon.crowdstrike.com/saml/metadata`
5. Contact our support team via our support portal to validate your IdP details. The information you provide to support must exactly match the information given by your application in your IdP, including these required attributes:
   - Entity ID (usually in the form of a URL)
   - Redirect URL
   - Public Certificate
   - Supported bindings

Issue: Unexpected Behavior with Internet Explorer, Edge, or Firefox

Use the Chrome browser to access Falcon and your IdP. Other browsers are unsupported.

Revision History

Version	Revision Date	Revision Details	Completed By
1.0	03/26/2018	Initial release of SSO for Falcon.	Scott P
1.1	03/29/2018	Added Okta, Ping screenshots and small corrections.	Scott P
1.2	07/26/2018	Improved instructions for AD FS	Scott P

CROWDSTRIKE TERMS AND CONDITIONS
(Signature Version 1-24-18)

These CrowdStrike Terms and Conditions by and between CrowdStrike, Inc., a Delaware corporation, on behalf of itself and any Affiliates performing hereunder (collectively, "**CrowdStrike**") with a principal place of business at 150 Mathilda Place, Suite 300, Sunnyvale, California 94086 and State of New Hampshire, with a principal place of business at 107 N Main St, Concord, New Hampshire 03301-4951 United States, is entered into as of the date signed by the last party (the "Effective Date").

These CrowdStrike Terms and Conditions are a master agreement that covers all CrowdStrike products and services but provisions regarding specific products or services apply only to the extent Customer has purchased, accessed or used such products or services.

1. Definitions.

"**Affiliate**" means any entity that a party directly or indirectly controls (e.g., subsidiary) or is controlled by (e.g., parent), or with which it is under common control (e.g., sibling).

"**Authorized Contractor**" means any individual or entity (other than a CrowdStrike Competitor) that has a written agreement to provide Customer services and is subject to confidentiality obligations covering CrowdStrike's Confidential Information and that is authorized hereunder to have access or use of a Product solely on behalf of and for Customer's Internal Use. Note that certain Products may not be used by Customer's Authorized Contractors. Customer's Authorized Contractors are subject to the terms and conditions herein and Customer remains responsible for their acts and omissions, and any breach by any such Authorized Contractor of the terms or conditions herein is a breach by Customer.

"**CrowdStrike Competitor**" means a person or entity in the business of developing, distributing, or commercializing Internet security products or services substantially similar to or competitive with CrowdStrike's products or services.

"**CrowdStrike Tool**" means any CrowdStrike proprietary software-as-a-service, software, hardware, or other tool that CrowdStrike uses in performing Professional Services, which may be specified in the applicable SOW. CrowdStrike Tools may include CrowdStrike's products.

"**Documentation**" means CrowdStrike's end-user technical documentation supplied with the applicable Offering.

"**Error**" means a reproducible failure of a Product to perform in substantial conformity with its applicable Documentation.

"**Internal Use**" means access or use solely for Customer's own internal information security purposes. By way of example and not limitation, Internal Use does not include access or use for the benefit of any person or entity other than Customer or for the development of any product or service. Internal Use is limited to access and use by Customer's employees unless this Agreement otherwise expressly authorizes use or access by Customer's Authorized Contractors, and in such case, solely on Customer's behalf and for Customer's benefit.

"**License/Access Term**" means the period of time during which Customer is authorized by CrowdStrike to access and use the Product or Product Related Service as set forth in the applicable Order.

"**Offerings**" means, collectively, any Products, Product-Related Services, or Professional Services.

"**Order**" means any purchase order or other ordering document (including any SOW) accepted by CrowdStrike or a reseller that identifies any Offering and any quantity thereof ordered by Customer based on CrowdStrike's applicable license metrics (e.g., number of endpoints (computers, laptops, desktops, and other devices), size of company (based on number of employees), number of file uploads, or number of queries). For an Order, only those transaction-specific terms detailing the Offerings ordered, quantity, price, payment terms, License/Access Term, and billing/provisioning contact information will have any force or effect unless a particular Order is executed by an authorized signer of CrowdStrike and returned to Customer (or the applicable reseller). If any such Order is so executed and delivered, then only those specific terms on the face of such Order that expressly identify those portions of this Agreement that are to be superseded will prevail over any conflicting terms herein but only with respect to those Offerings ordered on such Order. Orders are non-cancellable.

"**Product**" means any of CrowdStrike's cloud-based software or other products ordered by Customer as set forth in the relevant Order, including any Documentation and any Updates (as applicable) thereto that may be made available to Customer from time to time by CrowdStrike.

"**Product-Related Services**" means, collectively, (i) Falcon OverWatch; and (ii) the technical support services for certain Products provided by CrowdStrike -- either the standard support that is included with a Product during its License/Access Term or any additional support and/or support training options purchased as a separate SKU on an Order. Product-Related Services do not include Professional Services.

"**Professional Services**" means any professional services performed by CrowdStrike for Customer pursuant to an SOW or other Order. Professional Services may include without limitation incident response, investigation and forensic services related to cyber security adversaries, tabletop exercises, and next generation penetration tests related to cyber security.

"**Services**" means, collectively, any Product-Related Services and any Professional Services.

"**Statement of Work**" or "**SOW**" means a mutually-agreed executed written document describing the Professional Services to be performed by CrowdStrike for Customer, deliverables, fees, and expenses related thereto.

"**Updates**" means any correction, update, upgrade, patch, or other modification or addition made by CrowdStrike to any object code software component of a Product and made available to Customer by CrowdStrike from time to time.

2. Agreement Scope & Terms.

2.1 Entire Agreement. These CrowdStrike Terms and Conditions together with each Order (this "**Agreement**") constitute the entire agreement between Customer and CrowdStrike concerning the subject matter of this Agreement and it supersedes, and its terms govern, all prior proposals, agreements, understandings, or other communications between the parties, oral or written, regarding such subject matter.

2.2 Payment. Customer will pay the fees for Offerings as set forth in the applicable Order. Customer will pay the fees and amounts stated on each Order within 30 days after receipt of the applicable invoice (unless otherwise expressly set forth on the Order). All fees and other amounts are non-refundable (except as otherwise expressly provided in this Agreement) and exclusive of any applicable sales, use, value added, withholding, and other taxes, however designated, and Customer will pay all such taxes levied or imposed by reason of the transactions hereunder, except for taxes based on CrowdStrike's net income.

2.3 Affiliates and Resellers. Any Affiliate purchasing hereunder or using or accessing any Offering hereunder will be bound by and comply with all terms and conditions of this Agreement and Customer will remain responsible for Customer's Affiliates' acts and omissions unless Customer's Affiliate has entered into its own Terms and Conditions with CrowdStrike. Any Order through resellers is subject to, and CrowdStrike's obligations and liabilities to Customer are governed by, this Agreement.

3. Access & Use Rights.

3.1 Evaluation**.** If CrowdStrike approves Customer's evaluation use of a CrowdStrike product ("**Evaluation Product**"), the terms herein applicable to Products also apply to evaluation access and use of such Evaluation Product, except for the following different or additional terms: (a) the License/Access Term is as mutually agreed upon by Customer and CrowdStrike, provided that either CrowdStrike or Customer can terminate the evaluation at any time upon written (including email) notice to the other party; (b) the Evaluation Product is provided "AS-IS" without warranty of any kind, and CrowdStrike disclaims all warranties, support obligations, and other liabilities and obligations for the Evaluation Product; and (c) Customer's access and use is limited to Internal Use.

3.2 Access & Use Rights. Subject to the terms and conditions of this Agreement (including CrowdStrike's receipt of applicable fees), CrowdStrike grants Customer, under CrowdStrike's intellectual property rights in and to the applicable Product, a non-exclusive, non-transferable (except as expressly provided in Section 15.1 (Assignment)), non-sublicensable license to access and use the Products in accordance with any applicable Documentation solely for Customer's Internal Use during the applicable License/Access Term. Customer's access and use is limited to the quantity ordered in the applicable Order, which quantity is based on the license metric that applies to such Product (e.g., number of endpoints (such as computers, laptops, desktops, and other devices), size of company (based on number of employees), number of file uploads, or number of queries). Furthermore, the following additional terms and conditions apply to specific Products (or components thereof):

(a) Products with Object-Code Components. If Customer purchases a subscription to a Product with an object-code component ("**Software Component**"), Customer may, during the License/Access Term: (i) install and run multiple copies of the Software Components, respectively, solely for Customer's and Customer's Affiliates' Internal Use up to the maximum quantity based on the applicable license metric as ordered in the applicable Order; and (ii) allow Customer's Authorized Contractors to use and access the Software Component and associated Products solely on behalf, and for the benefit, of Customer and Customer's Affiliates.

(b) CrowdStrike Tools. If CrowdStrike provides CrowdStrike Tools to Customer pursuant to performing Professional Services, the license set forth in Section 3.2 (Access & Use Rights) applies to such CrowdStrike Tools as used solely for Customer's Internal Use during the period of time set forth in the applicable Order, or if none is specified, for the period authorized by CrowdStrike. Not all Professional Services engagements will involve delivery of CrowdStrike Tools.

(c) Restrictions. The access and use rights set forth in Section 3.2 (Access & Use Rights) do not include any rights to, and Customer will not, with respect to any Offering (or any portion thereof): (a) employ or authorize a CrowdStrike Competitor to use or view the Offering or Documentation, or to provide management, hosting, or support for an Offering; (b) alter, publicly display, translate, create derivative works of or otherwise modify an Offering; (c) sublicense, distribute or otherwise transfer an Offering to any third party (except as expressly provided in Section 15.1 (Assignment)); (d) allow third parties to access or use an Offering (except for Authorized Contractors as expressly permitted herein); (e) create public Internet "links" to an Offering or "frame" or "mirror" any Offering content on any other server or wireless or Internet-based device; (f) reverse engineer, decompile, disassemble or otherwise attempt to derive the source code (if any) for an Offering (except to the extent that such prohibition is expressly precluded by applicable law), circumvent its functions, or attempt to gain unauthorized access to an Offering or its related systems or networks; (g) use an Offering to circumvent the security of another party's network/information or develop malware; (h) remove or alter any notice of proprietary right appearing on an Offering; (i) conduct any benchmark or stress tests, competitive analysis on, or publish any performance data of, an Offering (provided, that this does not prevent Customer from comparing the Product to other products for Customer's Internal Use); (j) violate the Acceptable Use Policy; (k) use any feature of CrowdStrike APIs for any purpose other than in the performance of this Agreement; or (l) cause, encourage or assist any third party to do any of the foregoing. Customer agrees to use an Offering in accordance with laws, rules and regulations directly applicable to Customer and acknowledges that Customer is solely responsible for determining whether a particular use of an Offering is compliant with such laws.

(e) Installation and User Accounts. CrowdStrike is not responsible for installing Products unless Customer purchases installation services from CrowdStrike. For those Products requiring user accounts, only the single individual user assigned to a user account may access or use the Product. User accounts for Authorized Contractors may be established only for those Products permitting use or access by Authorized Contractors as described herein. Customer is liable and responsible for all actions and omissions occurring under Customer's and Customer's Authorized Contractor's user accounts for Offerings. Customer shall notify CrowdStrike if Customer learns of any unauthorized access or use of Customer's user accounts or passwords for an Offering.

(f) Malware Samples. If CrowdStrike makes malware samples available to Customer in connection with an evaluation or use of the Product ("**Malware Samples**"), Customer acknowledges and agrees that Customer's access to and use of Malware Samples is at Customer's own risk, that Customer has the requisite skill to safely handle Malware Samples, that Customer should not download or access any Malware Samples on or through its own production systems and networks and that doing so can infect and damage Customer's systems, networks, and data, and that Customer shall use the Malware Samples solely for evaluation of the Product and Internal Use and not for any malicious or unlawful purpose. CrowdStrike will not be liable for any loss or damage caused by any Malware Sample that may infect Customer's computer equipment, computer programs, data, or other proprietary material due to Customer's access to or use of the Malware Samples.

3.3 Third Party Software. CrowdStrike uses certain third party software in its Products, including what is commonly referred to as open source software. See the licensing terms and attributions for the third party software that CrowdStrike uses at: https://falcon.crowdstrike.com/opensource.

4. Cooperation & Services.

4.1 Cooperation**.** Customer authorizes CrowdStrike for purposes of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 et seq., Title III, 18 U.S.C. 2510 et seq., and the Electronic Communications Privacy Act, 18 U.S.C. § 2701 et seq. (and similar state, local and non-US laws) to access data and systems and process and transmit data through the Offerings.

4.2 Professional Services. Professional Services will commence on a mutually agreed upon date. Estimates provided for Professional Services performed on a time-and-material basis are estimates only and not a guaranteed time of completion. Professional Services performed on a fixed fee basis are limited to the scope of services stated in the applicable Order. Professional Services do not constitute works for hire and the only deliverable is a report consisting primarily of CrowdStrike's findings, recommendations, and adversary information. Customer owns the copy of the report (including without limitation, all of Customer's Confidential Information therein) delivered to Customer ("**Deliverable**"), subject to CrowdStrike's ownership of the CrowdStrike Materials. Customer agrees that relative to Customer, CrowdStrike exclusively owns any and all software (including object and source code), flow charts, algorithms, documentation, adversary information, report templates, know-how, inventions, techniques, models, CrowdStrike trademarks, ideas and any and all other works and materials developed hereunder (including without limitation all intellectual property rights therein and thereto) (the "**CrowdStrike Materials**") and that title shall remain with CrowdStrike. Upon payment in full of the amounts due hereunder for the applicable Professional Services and to the extent the CrowdStrike Materials are incorporated into (not just referenced in) the Deliverable(s), Customer shall have a perpetual, non-transferable (except as expressly provided in Section 15.1 (Assignment)), non-exclusive license to use the CrowdStrike Materials solely as a part of the Deliverable(s) for Customer's Internal Use.

5. Data Security and Privacy. See Exhibit A.

6. Ownership & Feedback. Products and Product-Related Services are made available or licensed, not sold. CrowdStrike owns and retains all right, title and interest (including all intellectual property rights) in and to the Offerings, except for any Deliverable. Any feedback or suggestions that Customer provides to CrowdStrike regarding its Offerings (e.g., bug fixes and features requests) is non-confidential and may be used by CrowdStrike for any purpose without acknowledgement or compensation; provided, Customer will not be identified publicly as the source of the feedback or suggestion.

7. Third Party Agreements. Customer is responsible for obtaining and maintaining all telecommunications, broadband, computer equipment, and services needed to access and use the Offerings and for paying all charges related thereto. Offerings may contain features designed to interface with applications or services provided or made available by third parties ("**Third Party Services**"). In order to use a feature in connection with a Third Party Service, Customer must have a license from the provider of the relevant Third Party Service. If the Third Party Services are no longer available or if the applicable third party provider no longer allows the Third Party Services to interface with an Offering, then such features will no longer be available or function with an Offering. CrowdStrike and the provider of the applicable Third Party Service disclaim all warranties, indemnities, obligations, and other liabilities in connection with any interface or integration with the Third Party Service. Further, CrowdStrike disclaims all warranties, indemnities, obligations, and other liabilities in connection with any Third Party Service**.**

8. Confidentiality.

8.1 Definitions. In connection with this Agreement, each party ("**Recipient**") may receive Confidential Information of the other party ("**Discloser**") or third parties to whom Discloser has a duty of confidentiality. "**Confidential Information**" means non-public information in any form and regardless of the method of acquisition that the Discloser designates as confidential to Recipient or should be reasonably known by the Recipient to be Confidential Information due to the nature of the information disclosed and/or the circumstances surrounding the disclosure. Confidential Information shall not include information that is: (i) in or becomes part of the public domain (other than by disclosure by Recipient in violation of this Agreement); (ii) previously known to Recipient without an obligation of confidentiality and demonstrable by the Recipient; (iii) independently developed by Recipient without use of Discloser's Confidential Information; or (iv) rightfully obtained by Recipient from third parties without an obligation of confidentiality.

8.2 Restrictions on Use. Except as allowed in Section 8.3 (Exceptions), Recipient shall hold Discloser's Confidential Information in strict confidence and shall not disclose any such Confidential Information to any third party, other than to its employees, and contractors, including without limitation, counsel, accountants, and financial advisors (collectively, "Representatives"), its Affiliates and their Representatives, subject to the other terms of this Agreement, and in each case who need to know such information and who are bound by restrictions regarding disclosure and use of such information comparable to and no less restrictive than those set forth herein. Recipient shall not use Discloser's Confidential Information for any purpose other than as set forth in this Agreement. Recipient shall take the same degree of care that it uses to protect its own confidential information of a similar nature and importance (but in no event less than reasonable care) to protect the confidentiality and avoid the unauthorized use, disclosure, publication, or dissemination of the Discloser's Confidential Information.

8.3 Exceptions. Recipient may disclose Discloser's Confidential Information: (a) to the extent required by applicable law or regulation; (b) pursuant to a subpoena or order of a court or regulatory, self-regulatory, or legislative body of competent jurisdiction; (c) in connection with any regulatory report, audit, or inquiry; or (d) where requested by a regulator with jurisdiction over Recipient. In the event of such a requirement or request, Recipient shall give Discloser prompt written notice of such requirement or request prior to such disclosure and a reasonable opportunity to review and comment upon the disclosure and request confidential treatment or a protective order pertaining thereto prior to making such disclosure. If CrowdStrike is legally required to respond to a third party request for information (including but not limited to a third party subpoena) or to provide documents, information or testimony in connection with a Professional Services engagement, Customer shall pay all of CrowdStrike's reasonable and actual out of pocket legal fees and expenses (as evidenced by reasonably detailed invoices) in connection therewith. If CrowdStrike's Professional Services employees are required to expend time in such efforts, Customer shall pay the then current list price Professional Services fees for actual hours worked in responding to such requirement.

8.4 Destruction. Upon Discloser's written request, Recipient shall use commercially reasonable efforts to destroy the Confidential Information and any copies or extracts thereof. However, Recipient, its Affiliates and their Representatives may retain any Confidential Information that: (a) they are required to keep for compliance purposes under a document retention policy or as required by applicable law, professional standards, a court, or regulatory agency; or (b) have been created electronically pursuant to automatic or ordinary course archiving, back-up, security, or disaster recovery systems or procedures; provided, however, that any such retained information shall remain

subject to this Agreement. Upon Discloser's request, Recipient will provide Discloser with written confirmation of destruction in compliance with this provision.

8.5 Equitable Relief. Each party acknowledges that a breach of this Section 8 (Confidentiality) shall cause the other party irreparable injury and damage. Therefore, each party agrees that those breaches may be stopped through injunctive proceedings in addition to any other rights and remedies which may be available to the injured party at law or in equity without the posting of a bond.

9. Warranties & Disclaimer.

9.1 No Warranty for Pre-Production Versions. Any pre-production feature or version of an Offering provided is *experimental* and provided "AS IS" without warranty of any kind and will not create any obligation for CrowdStrike to continue to develop, productize, support, repair, offer for sale, or in any other way continue to provide or develop any such feature or Offering. Customer agrees that its purchase is not contingent on the delivery of any future functionality or features, or dependent on any oral or written statements made by CrowdStrike regarding future functionality or features.

9.2 Product Warranty. If Customer has purchased a Product, CrowdStrike warrants to Customer during the applicable License/Access Term that the Product will operate without Error and that CrowdStrike has used industry standard techniques to prevent the Products at the time of delivery from injecting malicious software viruses into Customer's endpoints where the Products are installed. Customer must notify CrowdStrike of any warranty claim during the License/Access Term. Customer's sole and exclusive remedy and the entire liability of CrowdStrike for its breach of this warranty will be for CrowdStrike, at its own expense to do at least one of the following: (a) use commercially reasonable efforts to provide a work-around or correct such Error; or (b) terminate Customer's license to access and use the applicable non-conforming Product and refund the prepaid fee prorated for the unused period of the License/Access Term. CrowdStrike shall have no obligation regarding Errors reported after the applicable License/Access Term.

9.3 Services Warranty. CrowdStrike warrants to Customer that it will perform all Services in a professional and workmanlike manner consistent with generally accepted industry standards. Customer must notify CrowdStrike of any warranty claim for Services during the period the Services are being performed or within 30 days after the conclusion of the Services. Customer's sole and exclusive remedy and the entire liability of CrowdStrike for its breach of this warranty will be for CrowdStrike, at its option and expense, to (a) use commercially reasonable efforts to re-perform the non-conforming Services, or (b) refund the portion of the fees paid attributable to the non-conforming Services.

9.4 Exclusions. The express warranties do not apply if the applicable Product or Service (a) has been modified, except by CrowdStrike, (b) has not been installed, used, or maintained in accordance with this Agreement or Documentation, or (c) is non-conforming due to a failure to use an applicable Update. If any part of a Product or Service references websites, hypertext links, network addresses, or other third party locations, information, or activities, it is provided as a convenience only. CrowdStrike has no responsibility for third party services, products or content and does not endorse, authorize, approve, certify, maintain, or control them and does not guarantee the accuracy, completeness, efficacy, or timeliness of the information located within them.

9.5 No Guarantee. CUSTOMER ACKNOWLEDGES, UNDERSTANDS, AND AGREES THAT CROWDSTRIKE DOES NOT GUARANTEE OR WARRANT THAT IT WILL FIND, LOCATE, OR DISCOVER ALL OF CUSTOMER'S OR ITS AFFILIATES' SYSTEM THREATS, VULNERABILITIES, MALWARE, AND MALICIOUS SOFTWARE, AND CUSTOMER AND ITS AFFILIATES WILL NOT HOLD CROWDSTRIKE RESPONSIBLE THEREFOR.

9.6 Disclaimer. EXCEPT FOR THE EXPRESS WARRANTIES IN THIS SECTION 9, CROWDSTRIKE AND ITS AFFILIATES DISCLAIM ALL OTHER WARRANTIES, WHETHER EXPRESS, IMPLIED OR STATUTORY OR OTHERWISE. TO THE MAXIMUM EXTENT PERMITTED UNDER APPLICABLE LAW, CROWDSTRIKE AND ITS AFFILIATES AND SUPPLIERS SPECIFICALLY DISCLAIM ALL IMPLIED

WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON-INFRINGEMENT WITH RESPECT TO THE OFFERINGS AND CROWDSTRIKE TOOLS. THERE IS NO WARRANTY THAT THE OFFERINGS OR CROWDSTRIKE TOOLS WILL BE ERROR FREE, OR THAT THEY WILL OPERATE WITHOUT INTERRUPTION OR WILL FULFILL ANY OF CUSTOMER'S PARTICULAR PURPOSES OR NEEDS. THE OFFERINGS AND CROWDSTRIKE TOOLS ARE NOT FAULT-TOLERANT AND ARE NOT DESIGNED OR INTENDED FOR USE IN ANY HAZARDOUS ENVIRONMENT REQUIRING FAIL-SAFE PERFORMANCE OR OPERATION. NEITHER THE OFFERINGS NOR CROWDSTRIKE TOOLS ARE FOR USE IN THE OPERATION OF AIRCRAFT NAVIGATION, NUCLEAR FACILITIES, COMMUNICATION SYSTEMS, WEAPONS SYSTEMS, DIRECT OR INDIRECT LIFE-SUPPORT SYSTEMS, AIR TRAFFIC CONTROL, OR ANY APPLICATION OR INSTALLATION WHERE FAILURE COULD RESULT IN DEATH, SEVERE PHYSICAL INJURY, OR PROPERTY DAMAGE. Customer agrees that it is Customer's responsibility to ensure safe use of an Offering and CrowdStrike Tool in such applications and installations.

10. Indemnification.

10.1 CrowdStrike's Obligation. CrowdStrike shall at its cost and expense (a) defend and/or settle any claim brought against Customer by an unaffiliated third party alleging that an Offering infringes or violates that third party's intellectual property rights, and (b) pay, indemnify, and hold Customer harmless from any settlement of such claim or any damages finally awarded to such third party by a court of competent jurisdiction as a result of such claim; provided, that Customer: (x) gives CrowdStrike prompt written notice of such claim; (y) permits CrowdStrike to solely control and direct the defense or settlement of such claim (however, CrowdStrike will not settle any claim in a manner that requires Customer to admit liability or pay money without Customer's prior written consent); and (z) provides CrowdStrike all reasonable assistance in connection with the defense or settlement of such claim, at CrowdStrike's cost and expense. In addition, Customer may, at Customer's own expense, participate in defense of any claim.

10.2 Remedies. If a claim covered under this Section occurs or in CrowdStrike's opinion is reasonably likely to occur, CrowdStrike may at its expense and sole discretion (and if Customer's access and use of an Offering is enjoined, CrowdStrike will, at its expense): (a) procure the right to allow Customer to continue using the applicable Offering; (b) modify or replace the applicable Offering to become non-infringing; or (c) if neither (a) nor (b) is commercially practicable, terminate Customer's license or access to the affected portion of applicable Offering and refund a portion of the pre-paid, unused fees paid by Customer corresponding to the unused period of the License/Access Term.

10.3 Exclusions. CrowdStrike shall have no obligations under this Section if the claim is based upon or arises out of: (a) any modification to the applicable Offering not made by CrowdStrike; (b) any combination or use of the applicable Offering with or in any third party software, hardware, process, firmware, or data, to the extent that such claim is based on such combination or use; (c) Customer's continued use of the allegedly infringing Offering after being notified of the infringement claim or after being provided with a modified version intended to address such alleged infringement; (d) Customer's failure to use the Offering in accordance with the applicable Documentation; and/or (f) Customer's use of the Offering outside the scope of the rights granted under this Agreement.

10.4 Exclusive Remedy. THE REMEDIES SPECIFIED IN THIS SECTION CONSTITUTE CUSTOMER'S SOLE AND EXCLUSIVE REMEDIES, AND CROWDSTRIKE'S ENTIRE LIABILITY, WITH RESPECT TO ANY INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

11. **Limitation of Liability.** TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, EXCEPT FOR LIABILITY FOR ANY AMOUNTS PAID OR PAYABLE TO THIRD PARTIES UNDER SECTION 10 (INDEMNIFICATION), CUSTOMER'S PAYMENT OBLIGATIONS, AND/OR ANY INFRINGEMENT OR MISAPPROPRIATION BY ONE PARTY OF THE OTHER PARTY'S INTELLECTUAL PROPERTY RIGHTS, NEITHER PARTY SHALL BE LIABLE TO THE OTHER PARTY IN CONNECTION WITH THIS AGREEMENT OR THE SUBJECT MATTER HEREOF (UNDER ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STATUTE, TORT OR OTHERWISE) FOR: (a) ANY LOST PROFITS, LOST BUSINESS OPPORTUNITIES, LOST DATA, OR SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE

DAMAGES, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES OR SUCH DAMAGES OR LOSSES WERE REASONABLY FORESEEABLE; OR (b) AN AMOUNT THAT EXCEEDS THE TOTAL FEES PAID OR PAYABLE TO CROWDSTRIKE FOR THE RELEVANT OFFERING DURING THE TWELVE-MONTH PERIOD BEFORE THE EVENT GIVING RISE TO SUCH LIABILITY. THESE LIMITATIONS WILL APPLY NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SPECIFIED IN THIS AGREEMENT. MULTIPLE CLAIMS SHALL NOT EXPAND THE LIMITATIONS SPECIFIED IN THIS SECTION.

12. **Compliance with Laws.** Each party agrees to comply with all U.S. federal, state, local and non-U.S. laws directly applicable to such party in the performance of this Agreement, including applicable export and import laws. Customer acknowledges and agrees the Product shall not be used, transferred, or otherwise exported or re-exported to countries as to which the United States and/or the European Union maintains an embargo (collectively, "Embargoed Countries"), or to or by a national or resident thereof, or any person or entity on the U.S. Department of Treasury's List of Specially Designated Nationals or the U.S. Department of Commerce's Table of Denial Orders (collectively, "Designated Nationals"). Customer represents and warrants that Customer is not located in, or is under the control of, or a national or resident of, an Embargoed Country or Designated National.

13. **U.S. Government End Users**. The Products and Documentation are "commercial items," as that term is defined in FAR (48 C.F.R.) 2.101, consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in FAR 12.211 and 12.212. Consistent with FAR 12.211 and 12.212 and DFARS (48 C.F.R.) 227.7202-1 through 227.7202-4, the Products and Documentation are being licensed to U.S. government end users under the license(s) customarily provided to the public as forth in this Agreement. If this Agreement fails to meet the Government's needs or is inconsistent in any way with Federal law, and the parties cannot reach a mutual agreement on terms for this Agreement, the Government agrees to terminate its use of the Products and Services and return the Products and Services and any other software or technical data delivered as part of the Products and Services, unused, to CrowdStrike. In addition, DFARS 252.227-7015 (Technical Data – Commercial Items) applies to technical data acquired by Department of Defense agencies. This U.S. Government Rights clause in this Section is in lieu of, and supersedes, any other FAR, DFARS, or other clause, provision, or supplemental regulation that addresses Government rights in computer software or technical data under this Agreement.

14. **Termination.** This Agreement shall remain effective until termination in accordance with this Section or as otherwise specified herein. If Customer materially breaches Section 3.2 (Access and Use Rights) of this Agreement or fail to pay CrowdStrike on time (and fail to cure such material breach in accordance herewith), in addition to all other rights and remedies that CrowdStrike may have at law or in equity, CrowdStrike may, without terminating this Agreement, and in its sole discretion and without further notice to Customer, suspend Customer's access or use of the Offerings. Either party may terminate this Agreement: (a) upon 30 days' written notice of a material breach by the other party, unless the breach is cured within the 30-day notice period; or (b) immediately, if the other party ceases to do business, becomes insolvent, or seeks protection under any bankruptcy or comparable proceedings. Upon termination of this Agreement for any reason: (i) all Customer's access and use rights granted in this Agreement will immediately terminate; (ii) Customer must promptly cease all use of Offerings and de-install all Software Components installed on Customer's endpoints; and (iii) data retention is based on the retention parameters that Customer has purchased for the applicable Product and such data will be deleted in accordance with such parameters. Sections 1 (Definitions), _____(c) (Access and Use Right - Restrictions), 6 (Ownership and Feedback), 8 (Confidentiality), 10 (Indemnification), 11 (Limitation of Liability), 14 (Termination), and 15 (General) and all liabilities that accrue prior to termination shall survive expiration or termination of this Agreement for any reason.

15. General.

15.1 Assignment. Neither party may assign this Agreement without the prior written consent of the other party, except to an Affiliate in connection with a corporate reorganization or in connection with a merger, acquisition, or sale of all or substantially all of its business and/or assets. Any assignment in violation of this Section shall be void. Subject to the foregoing, all rights and obligations of the parties under this Agreement shall be binding upon and inure to the benefit of and be enforceable by and against the successors and permitted assigns.

15.2 Governing Law; Venue. Except as otherwise provided in Exhibit B (if applicable), this Agreement, and the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced in accordance with the laws of the State of California, excluding its conflicts-of-law principles. The sole and exclusive jurisdiction and venue for actions arising under this Agreement shall be state and federal courts in Santa Clara County, California, and the parties agree to service of process in accordance with the rules of such courts. The Uniform Computer Information Transactions Act and the United Nations Convention on the International Sale of Goods shall not apply. Notwithstanding the foregoing, each party reserves the right to file a suit or action in any court of competent jurisdiction as such party deems necessary to protect its intellectual property rights and, in CrowdStrike's case, to recoup any payments due.

15.3 Independent Contractors; No Third Party Rights. The parties are independent contractors. This Agreement shall not establish any relationship of partnership, joint venture, employment, franchise, or agency between the parties. No provision in this Agreement is intended or shall create any rights with respect to the subject matter of this Agreement in any third party.

15.4 Waiver & Severability; Amendments; Order of Precedence The failure of either party to enforce any provision of this Agreement shall not constitute a waiver of any other provision or any subsequent breach. If any provision of this Agreement is held to be illegal, invalid, or unenforceable, the provision will be enforced to the maximum extent permissible so as to affect the intent of the parties, and the remaining provisions of this Agreement will remain in full force and effect. This Agreement may only be amended, or any term or condition set forth herein waived, by written consent of both parties. If there is a conflict between the terms contained in the main body of this Agreement and any SOW, the terms in the main body will prevail over the terms in a SOW.

15.5 Force Majeure. Neither party shall be liable for, nor shall either party be considered in breach of this Agreement due to, any failure to perform its obligations under this Agreement (other than its payment obligations) as a result of a cause beyond its control, including but not limited to, act of God or a public enemy, act of any military, civil or regulatory authority, change in any law or regulation, fire, flood, earthquake, storm or other like event, disruption or outage of communications (including an upstream server block and Internet or other networked environment disruption or outage), power or other utility, labor problem, or any other cause, whether similar or dissimilar to any of the foregoing, which could not have been prevented with reasonable care.

15.6 Notices. All legal notices will be given in writing to the addresses below and will be effective (a) when personally delivered, (b) on the reported delivery date if sent by a recognized international or overnight courier, or (c) five business days after being sent by registered or certified mail (or ten days for international mail). For clarity, Orders, POs, and other documents relating to order processing and payment are not legal notices and may be delivered electronically in accordance with each party's standard ordering procedures.

15.7 Signatures. This Agreement and any SOWs may be executed in two counterparts, each of which will be considered an original but all of which together will constitute one agreement. Any signature delivered by electronic means shall be treated for all purposes as an original.

CROWDSTRIKE, INC.		**STATE OF NEW HAMPSHIRE**	
By:	_____	By:	_____
Name:	_____	Name:	_____
Title:	_____	Title:	_____
Date:	_____	Date:	_____

Exhibit A: Data Security and Privacy Schedule

1. **Definitions**.

a. "**CrowdStrike Systems**" means those computer systems hosting the 'Falcon EPP Platform'.

b. **"Execution Profile/Metric Data"** means any machine-generated data, such as metadata derived from tasks, file execution, commands, resources, network telemetry, executable binary files, scripts, and processes, that Customer provides to CrowdStrike in connection with this Agreement or that is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data to the extent that it includes Personal Data for which Customer is responsible. Customer, rather than CrowdStrike, determines which types of data, whether Personal Data or not, exist on its systems. Accordingly, Customer's endpoint environment is unique in configurations and naming conventions and the machine event data could potentially include Personal Data.

c. "**Personal Data**" means information used to distinguish or trace a natural person's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific natural person. Personal Data also includes such other information about a specific natural person to the extent that the data protection laws applicable in the jurisdictions in which such person resides define such information as Personal Data.

d. "**Privacy and Security Laws**" means U.S. federal, state and local and non-U.S. laws that regulate the privacy or security of Personal Data and that are directly applicable to CrowdStrike.

e. "**Process or Processing**" means the collection, access to, use, storage, disclosure, transfer, or other processing of Personal Data of any natural person whom Customer authorizes to use or access an Offering.

f. "**Security Incident**" means unauthorized access to, or unauthorized acquisition of, Personal Data stored on CrowdStrike Systems that results in the compromise of Personal Data for which Customer is responsible.

g. "**Threat Actor Data**" means any malware, spyware, virus, worm, Trojan horse, or other potentially malicious or harmful code or files, URLs, DNS data, network telemetry, commands, processes or techniques, metadata, or other information or data, in each case that is potentially related to unauthorized third parties associated therewith and that (i) Customer provides to CrowdStrike in connection with this Agreement, or (ii) is collected or discovered during the course of CrowdStrike providing Offerings, excluding any such information or data to the extent that it includes Personal Data for which Customer is responsible.

2. **Falcon Platform**

The 'Falcon EPP Platform' uses a crowd-sourced environment, for the benefit of all customers, to protect customers against suspicious and potentially destructive activities. CrowdStrike's Products are designed to detect, prevent, respond to, and identify intrusions by collecting and analyzing data, including machine event data, executed scripts, code, system files, log files, dll files, login data, binary files, tasks, resource information, commands, protocol identifiers, URLs, network data, and/or other executable code and metadata. CrowdStrike uses the data to analyze, characterize, attribute, warn of, and/or respond to threats against Customer and other customers, analyze trends and performance, improve the functionality of, and develop, CrowdStrike's products and services, and enhance cybersecurity. Neither Execution Profile/Metric Data nor Threat Actor Data are Customer's Confidential Information.

3. **Processing Personal Data**.

a. Provisioning/Use of Offerings**.** Personal Data may be collected and used during the provisioning and use of the Offerings to deliver, support and improve the Offerings, administer the Agreement and further the business relationship between Customer and CrowdStrike, comply with law, act in accordance with Customer's written instructions, or otherwise in accordance with this Agreement. Customer authorizes CrowdStrike to collect, use, store, and transfer the Personal Data that Customer provides to CrowdStrike as contemplated in this Agreement.

b. Suspicious/Unknown File Analysis. While using certain CrowdStrike Offerings Customer may have the option to upload (by submission, configuration, and/or, in the case of Services, by CrowdStrike personnel retrieval) files and other information related to the files for security analysis and response or, when submitting crash reports, to make the product more reliable and/or improve CrowdStrike's products and services or enhance cybersecurity. These potentially suspicious or

unknown files may be transmitted and analyzed to determine functionality and their potential to cause instability or damage Customer's endpoint. In some instances, these files could contain Personal Data for which Customer is responsible.

4. Compliance with Privacy and Information Security Requirements

a. Compliance with Laws. CrowdStrike shall comply with all Privacy and Security Laws and the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of Personal Data from the European Economic Area. In addition, CrowdStrike shall comply with the U.S. - Swiss Safe Harbor framework or its successor as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data from Switzerland. CrowdStrike's privacy notice may be found at http://www.crowdstrike.com/privacy-notice/. To the extent that Customer is a controller of Personal Data originating in the European Union or Switzerland, the Data Protection Addendum set forth on the portal shall apply to CrowdStrike's processing of such Personal Data.

b. Safeguards. CrowdStrike shall maintain appropriate technical and organizational safeguards commensurate with the sensitivity of the Personal Data processed by it on Customer's behalf, which are designed to protect the security, confidentiality, and integrity of such Personal Data and protect such Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, including the safeguards set forth on Appendix A which substantially conform to the ISO/IEC 27002 control framework. ("Information Security Controls for CrowdStrike Systems").

c. Access; Contacts. With respect to employees, agents, and subcontractors, CrowdStrike shall limit access to Personal Data to only those employees, agents, and subcontractors who have a need to access the Personal Data in order to provide, support, and improve the Products and Services. CrowdStrike shall assign and train personnel who shall: (i) liaise with customers regarding any issues concerning the security of Personal Data; (ii) receive notice of any Security Incident discovered by CrowdStrike and provide notice of any such Security Incident to Customer; and (iii) coordinate CrowdStrike's Security Incident response and remedial action.

5. **Security Incident Response**. In the event CrowdStrike discovers a Security Incident, CrowdStrike shall:

a. Promptly notify Customer of the discovery of the Security Incident. Such notice shall summarize the known circumstances of the Security Incident and the corrective action taken or to be taken by CrowdStrike.

b. Conduct an investigation of the circumstances of the Security Incident.

c. Use commercially reasonable efforts to remediate the Security Incident.

d. Use commercially reasonable efforts to communicate and cooperate with Customer concerning its response to the Security Incident.

6. **Provision of SOC II, Type 2 Report and SIG**. Promptly after written (including email) request from Customer, CrowdStrike shall provide Customer with: (1) its most recent SOC II, Type 2 report regarding the CrowdStrike Systems; and (2) provide its completed Standardized Information Gathering (SIG) questionnaire for the CrowdStrike Systems.

7. **Security Assessment**. Upon the provision of reasonable notice to CrowdStrike, once every twelve months during the term of the Agreement and during normal business hours unless otherwise decided by CrowdStrike in its sole discretion, CrowdStrike shall make appropriate CrowdStrike personnel reasonably available to Customer to discuss CrowdStrike's manner of compliance with applicable security obligations under this Agreement. In advance of such discussion, CrowdStrike may, in its sole discretion, provide Customer with access to information or documentation concerning CrowdStrike's information security practices as they relate to this Agreement, including without limitation, access to any security assessment reports designed to be shared with third parties. Any information or documentation provided pursuant to this assessment process or otherwise pursuant to this Schedule shall be considered CrowdStrike's Confidential Information and subject to the Confidentiality section of the Agreement.

8. **Customer Obligations**. Customer confirms that it has a lawful basis in having CrowdStrike process the Personal Data and/or that Customer has made such disclosures and obtained such consents and authorizations for the lawful processing of Personal Data by CrowdStrike.

9. **Notices**. The following individuals shall be the primary contacts at Customer and CrowdStrike for any coordination, communications or notices with respect to Personal Data and this Schedule:

   a. CrowdStrike: Drew Bagley, Senior Privacy Counsel (drew.bagley@crowdstrike.com with a copy to legal@crowdstrike.com). For any Security Incident: Jerry Dixon, Chief Information Security Officer (jerry.dixon@crowdstrike.com with a copy to security@crowdstrike.com).
   b. Customer: the person who has signed the Agreement or another person as otherwise designated in writing (including by email) by Customer to CrowdStrike. Each party shall promptly notify the other if any of the foregoing contact information changes.

Appendix A
Information Security Controls for CrowdStrike Systems

Security Control Category	Description
1. Governance	**a.** Assign to an individual or a group of individuals appropriate roles for developing, coordinating, implementing, and managing CrowdStrike's administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Personal Data **b.** Use of data security personnel that are sufficiently trained, qualified, and experienced to be able to fulfill their information security-related functions
2. Risk Assessment	a. Conduct periodic risk assessments designed to analyze existing information security risks, identify potential new risks, and evaluate the effectiveness of existing security controls b. Maintain risk assessment processes designed to evaluate likelihood of risk occurrence and material potential impacts if risks occur c. Document formal risk assessments d. Review formal risk assessments by appropriate managerial personnel
3. Information Security Policies	**a.** Create information security policies, approved by management, published and communicated to all employees and relevant external parties. **b.** Review policies at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.
4. Human Resources Security	a. Maintain policies requiring reasonable background checks of any new employees who will have access to Personal Information or relevant CrowdStrike Systems, subject to local law b. Regularly and periodically train personnel on information security controls and policies that are relevant to their business responsibilities and based on their roles within the organization
5. Asset Management	a. Maintain policies establishing data classification based on data criticality and sensitivity b. Maintain policies establishing data retention and secure destruction requirements c. Implement procedures to clearly identify assets and assign ownership
6. Access Controls	a. Identify personnel or classes of personnel whose business functions and responsibilities require access to Personal Information, relevant CrowdStrike Systems and the organization's premises b. Maintain controls designed to limit access to Personal Information, relevant CrowdStrike Systems and the facilities hosting the CrowdStrike Systems to authorized personnel c. Review personnel access rights on a regular and periodic basis d. Maintain physical access controls to facilities containing CrowdStrike Systems, including by using access cards or fobs issued to CrowdStrike personnel as appropriate e. Maintain policies requiring termination of physical and electronic access to Personal Information and CrowdStrike Systems after termination of an employee f. Implement access controls designed to authenticate users and limit access to CrowdStrike Systems g. Implement policies restricting access to the data center facilities hosting CrowdStrike Systems to approved data center personnel and limited and approved CrowdStrike personnel h. Maintain dual layer access authentication processes for CrowdStrike employees with administrative access rights to CrowdStrike Systems
7. Cryptography	a. Implement encryption key management procedures b. Encrypt sensitive data using a minimum of AES/128 bit ciphers in transit and at rest
8. Physical Security	a. Require two factor controls to access office premises b. Register and escort visitors on premises

9. Operations Security	a. Perform periodic network and application vulnerability testing using dedicated qualified internal resources b. Contract with qualified independent 3rd parties to perform periodic network and application penetration testing c. Implement procedures to document and remediate vulnerabilities discovered during vulnerability and penetration tests
10. Communications Security	a. Maintain a secure boundary using firewalls and network traffic filtering b. Require internal segmentation to isolate critical systems from general purpose networks c. Require periodic reviews and testing of network controls
11. System Acquisition, Development and Maintenance	a. Assign responsibility for system security, system changes and maintenance b. Test, evaluate and authorize major system components prior to implementation
12. Supplier Relationships	Periodically review available security assessment reports of vendors hosting the CrowdStrike Systems to assess their security controls and analyze any exceptions set forth in such reports
13. Information Security Incident Management	a. Monitor the access, availability, capacity and performance of the CrowdStrike Systems, and related system logs and network traffic using various monitoring software and services b. Maintain incident response procedures for identifying, reporting, and acting on Security Incidents c. Perform incident response table-top exercises with executives and representatives from across various business units d. Implement plan to address gaps discovered during exercises e. Establish a cross-disciplinary Security Incident response team
14. Business Continuity Management	a. Design business continuity with goal of 99.9% uptime SLA b. Conduct scenario based testing annually
15. Compliance	a. Establish procedures designed to ensure all applicable statutory, regulatory and contractual requirements are adhered to

Exhibit B
Dispute Resolution Outside North America

If Customer's principal office is located outside North America as indicated in the Agreement, the terms and conditions of this Exhibit shall apply to all disputes arising out of or relating to this Agreement (excluding disputes regarding the actual or alleged violation of CrowdStrike's intellectual property rights or the collection of overdue invoices, which shall be governed by California law).

1. ***For ALL principal offices outside North America:***

a. Choice of Law. This Agreement, and the rights and duties of the parties arising from this Agreement, shall be governed by, construed, and enforced with the laws of the State of New York, excluding its conflicts-of-law principles. The Uniform Computer Information Transactions Act and the United Nations Convention on the International Sale of Goods shall not apply.

b. Arbitration. Any dispute, claim, or controversy arising out of or relating to this Agreement or the existence, breach, termination, enforcement, interpretation, or validity of the Agreement, including the determination of the scope or applicability of this Agreement to arbitrate, (each, a "**Dispute**") shall be referred to and finally resolved by arbitration under the rules and at the location identified below. The arbitral panel shall consist of three (3) arbitrators, selected as follows: each party shall appoint one (1) arbitrator; and those two (2) arbitrators shall discuss and select third arbitrator. If the two party-appointed arbitrators are unable to agree on a third arbitrator, the third arbitrator shall be selected in accordance with the applicable rules of the arbitration body. Each arbitrator shall be independent of each of the parties and shall have suitable experience and knowledge in the subject matter of the Dispute. The arbitrators shall have the authority to grant specific performance and to allocate between the parties the costs of arbitration (including service fees, arbitrator fees and all other fees related to the arbitration) in such equitable manner as the arbitrators may determine. Judgment upon the award so rendered may be entered in a court having jurisdiction or application may be made to such court for judicial acceptance of any award and an order of enforcement, as the case may be. Notwithstanding the foregoing, either party shall have the right to institute an action in a court of proper jurisdiction for preliminary injunctive relief pending a final decision by the arbitrator, provided that a permanent injunction and damages shall only be awarded by the arbitrator. The language to be used in the arbitral proceedings shall be English.

2. ***For ONLY principal offices within Europe, the Middle East or Africa:***

Any Dispute shall be referred to and finally resolved by arbitration under the London Court of International Arbitration Rules (which Rules are deemed to be incorporated by reference into this clause) on the basis that the governing law is the law of the State of New York, USA. The seat, or legal place, of arbitration shall be London, England.

3. ***For ONLY principal offices within Asia Pacific, Australia & New Zealand:***

Any Dispute shall be referred to and finally resolved by arbitration under the Rules of Conciliation and Arbitration of the International Chamber of Commerce in force on the date when the notice of arbitration is submitted in accordance with such Rules (which Rules are deemed to be incorporated by reference into this clause) on the basis that the governing law is the law of the State of New York, USA. The seat, or legal place, of arbitration shall be Singapore.

4. ***For ONLY principal offices within the Americas, excluding North America:***

Any Dispute shall be referred to and finally resolved by arbitration under International Dispute Resolution Procedures of the American Arbitration Association in force on the date when the notice of arbitration is submitted in accordance with such Procedures (which Procedures are deemed to be incorporated by reference into this clause) on the basis that the governing law is the law of the State of New York, USA. The seat, or legal place, of arbitration shall be New York, New York, USA.

ORACLE ORDER FORM FOR DYN SERVICES

Business Name ("Client"): State of New Hampshire, Office of Secretary of State

Offer Presented By: Jillian D'Anna
Offer Expires: 2018-10-31
Effective Date:
Initial Term: 1 Months
Renewal Terms: 0 Months

Client Information

Sold To Contact:

Name: David Scanlan
Address: State House, Room 204
107 North Main Street Concord NH 03301
United States
Email: david.scanlan@sos.nh.gov
Phone: (603) 271-3242

Invoice Contact:

Name:
Address:
United States
Email:
Phone:

Services	One-Time Fees	Recurring Fees	Overage Fees (if applicable)
Dyn Enterprise WAF (GB)	-		-
1 Endpoint(s)	-		$100 per Endpoint
Enterprise WAF Subscription	-		-
3,000 GB of Traffic	-		$0.27000 per GB
Gold Level Support for WAF	-		-
100,000,000 Requests	-		$0.90000 per Million Requests
1 Internet Intelligence Network	-		-
Managed DNS Service	-		-
1,000 Domains	-		-
1,000 Dynamic DNS	-		-
5 QPS	-		$100 per QPS
25,000 Resource Records	-		-
Total Fees (Quarterly) In Arrears (USD)	**$0**	**$1,500**	

Special Notes

Oracle will waive any Overage Fee(s) assessed to Client for the three (3) months immediately following the effective date of this order form

Terms and Conditions: Client agrees to be bound by the terms of this Order Form and the terms of the Master Services Agreement, Product Specific Terms and Conditions, and Acceptable Use Policy located at http://dyn.com/legal/enterprise-legal-terms/. If an effective date is not specified above, then the effective date of this Order shall be the date of Client's signature below.

Client's Authorized Signature
Name: David Scanlan
Title:
Date:

Oracle America, Inc.'s Authorized Signature
Name: Jesse Lanard McNair
Title:
Date:

ORACLE CLIENT PAYMENT INFORMATION FORM

Payment Information

Please select your payment method and fill out the appropriate information below. In the event Client desires to remit payments to Oracle via Check or Wire Transfer, Client may be asked to provide additional information so that the Client's business can be evaluated for the extension of credit. Payment terms are Net 30 unless otherwise noted on this Order Form.

☐ Credit Card **(Payments Due Upon Receipt. Additional information required below.)**

☐ Check **(Make checks payable to Oracle America, Inc.)**

☐ Wire **(Wire fees may apply where the wire originates outside of the United States.)**

ALL PAYMENTS MUST BE MADE IN US DOLLARS

Credit Card Information:

If you elected to make payments via credit card, please provide the required account information below.

IMPORTANT: Oracle uses an electronic document process to help protect the security of your financial information. If you are completing this form outside of this process, do not write your credit card information onto the downloaded form. Instead, contact Oracle's billing team (+1 603-663-0303 or billing@dyn.com) to arrange an alternative method.

Credit Card Information

Name (as displayed on Credit Card):		
Credit Card Number:	Credit Card Type:	Exp. Date: ____ /_____
Billing Address:		

Purchase Orders: If Client's business practices require a purchase order number be used prior to payment of any invoices, Client must indicate so by checking the box and providing the applicable purchase order number below. Please send all Purchase Orders to billing@dyn.com.

Purchase Order Number Required: ☐ Purchase Order Number:_____

By signing this Client Payment Information Form, Client authorizes Oracle to charge the above referenced account(s) any fees due under each Order Form entered into by and between Oracle and Client.

_____ _____

Client's Authorized Representative **Title**

David Scanlan _____

Print Name **Date**

ORACLE ORDER FORM FOR DYN SERVICES

Business Name ("Client"): State of New Hampshire, Office of Secretary of State

Offer Presented By: Jillian D'Anna
Offer Expires: 2018-10-31
Effective Date:
Initial Term: 1 Months
Renewal Terms: 0 Months

Client Information

Sold To Contact:

Name: David Scanlan
Address: State House, Room 204
107 North Main Street Concord New Hampshire 03301 United States
Email: elections@sos.nh.gov
Phone: (603) 271-3242

Invoice Contact:

Name:
Address:
United States
Email:
Phone:

Services	One-Time Fees	Recurring Fees	Overage Fees (if applicable)
Dyn Enterprise WAF (GB)	-		-
1 Endpoint(s)	-		$100 per Endpoint
Enterprise WAF Subscription	-		-
20 GB of Traffic	-		$0.27000 per GB
Gold Level Support for WAF	-		-
100,000,000 Requests	-		$0.90000 per Million Requests
1 Internet Intelligence Network	-		-
Managed DNS Service	-		-
1,000 Domains	-		-
1,000 Dynamic DNS	-		-
5 QPS	-		$100 per QPS
25,000 Resource Records	-		-
Total Fees (Quarterly) In Arrears (USD)	**$0**	**$1,500**	

Special Notes

Terms and Conditions: Client agrees to be bound by the terms of this Order Form and the terms of the Master Services Agreement, Product Specific Terms and Conditions, and Acceptable Use Policy located at http://dyn.com/legal/enterprise-legal-terms/. If an effective date is not specified above, then the effective date of this Order shall be the date of Client's signature below.

Client's Authorized Signature
Name: David Scanlan
Title:
Date:

Oracle America, Inc.'s Authorized Signature
Name: Jesse Lanard McNair
Title:
Date:

ORACLE CLIENT PAYMENT INFORMATION FORM

Payment Information

Please select your payment method and fill out the appropriate information below. In the event Client desires to remit payments to Oracle via Check or Wire Transfer, Client may be asked to provide additional information so that the Client's business can be evaluated for the extension of credit. Payment terms are Net 30 unless otherwise noted on this Order Form.

☐ Credit Card **(Payments Due Upon Receipt. Additional information required below.)**

☐ Check **(Make checks payable to Oracle America, Inc.)**

☐ Wire **(Wire fees may apply where the wire originates outside of the United States.)**

ALL PAYMENTS MUST BE MADE IN US DOLLARS

Credit Card Information:

If you elected to make payments via credit card, please provide the required account information below.

IMPORTANT: Oracle uses an electronic document process to help protect the security of your financial information. If you are completing this form outside of this process, do not write your credit card information onto the downloaded form. Instead, contact Oracle's billing team (+1 603-663-0303 or billing@dyn.com) to arrange an alternative method.

Credit Card Information

Name (as displayed on Credit Card):		
Credit Card Number:	Credit Card Type:	Exp. Date: ____ /_____
Billing Address:		

Purchase Orders: If Client's business practices require a purchase order number be used prior to payment of any invoices, Client must indicate so by checking the box and providing the applicable purchase order number below. Please send all Purchase Orders to billing@dyn.com.

Purchase Order Number Required: ☐ Purchase Order Number:_____

By signing this Client Payment Information Form, Client authorizes Oracle to charge the above referenced account(s) any fees due under each Order Form entered into by and between Oracle and Client.

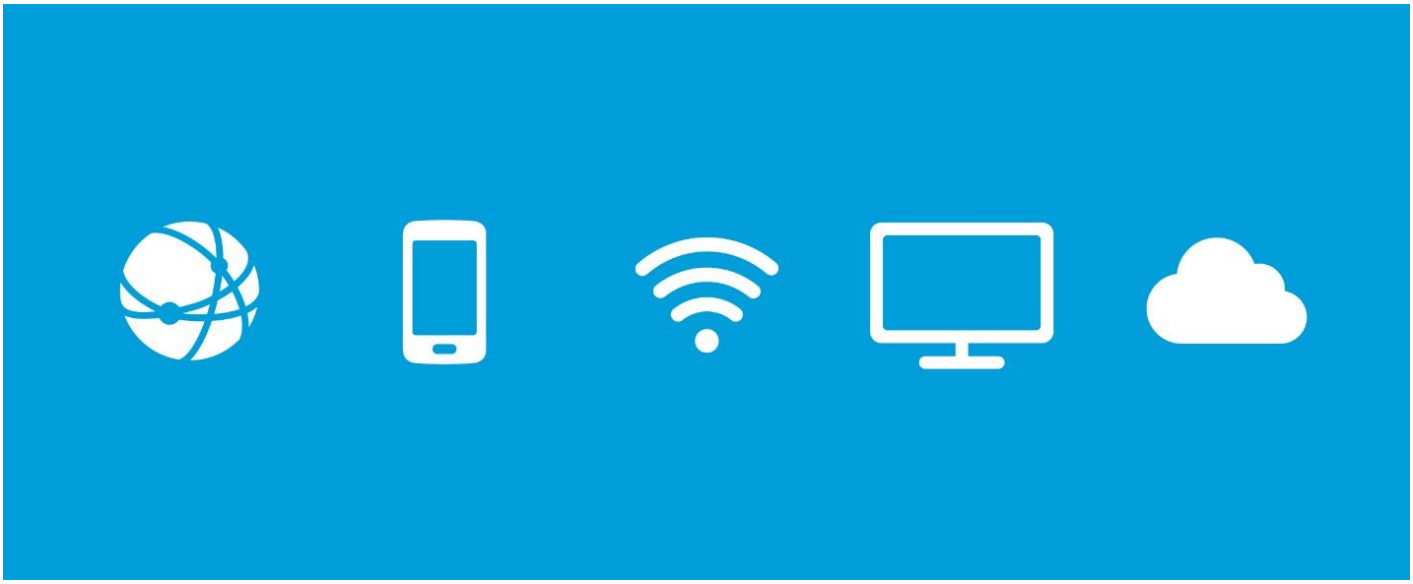
_____ _____

Client's Authorized Representative **Title**

David Scanlan _____

Print Name **Date**

AT&T Response to State of New Hampshire's RFI for Cybersecurity Assessment



AT&T

003607

1500 S. Willow ST, 1ST FL
Manchester NH 03103

Office: 888-308-5270
Mobile: 508-308-9996
todd.theel@att.com
www.att.com

June 01, 2018

Daniel J. Dister
Chief Information Security Officer
State of New Hampshire, Department of Information Technology
61-65 S Spring St,
Concord, NH 03301
Daniel.Dister@doit.nh.gov

Re: DoIT Cybersecurity Assessment RFI

Dear Mr. Dister:

As the State of New Hampshire, Department of Information Technology (DoIT) continues to grow, it's faced with numerous challenges. Your business relies on communication services to conduct day-to-day business but coordinating these services can be a daunting task.

AT&T Cybersecurity Consulting understands your priorities and the initiatives that are driving change within your organization. After carefully reviewing your requirements, we designed a solution to deliver a comprehensive security review and assessment of your security environment. Our proposed solution offers you

- Assess security risks and understand potential breach points
- Benchmark enterprise security posture
- Increase visibility security risks and provide actionable recommendations for enterprise security

AT&T Cybersecurity Consulting provides a unique and world-class portfolio of assessment, compliance and related security services. Our experience, expertise, and commitment to open standards have established us as a strategic and trusted advisor. By leveraging AT&T, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to address your information protection and compliance needs.

We look forward to working with DoIT on this important initiative. If you have any questions regarding this submission, please do not hesitate to contact me at (888) 308-5270.

Sincerely,

Todd Theel

Richard Nadzum

Todd A. Theel
Client Solutions Executive 2

Richard Nadzum
Business Development Manager 1

Connecting Your World

AT&T Response to State of New Hampshire's RFI for Cybersecurity Assessment

June 01, 2018

Todd A. Theel
AT&T
Client Solutions Executive 2
1500 S. Willow ST,1ST FL
Manchester NH 03103
Office: 888-308-5270
Mobile: 508-308-9996
todd.theel@att.com

Table of Contents

1. Executive Summary

AT&T Cybersecurity Consulting is pleased to present our response to the State of New Hampshire, Department of Information Technology's RFI for Cybersecurity Assessment. Based on this RFI, it is the understanding of AT&T Cybersecurity Consulting that State of New Hampshire, Department of Information Technology (DoIT) seeks a qualified partner to help strengthen its current security posture by providing ongoing IT and physical security vulnerability assessment services. These services are intended to test and review the networks, devices, applications, and policy/process environment for potential security vulnerabilities, compliance related issues, and opportunities for improvement. Though our unified approach to information security and compliance, AT&T Cybersecurity Consulting can help DoIT define, and then execute upon, a unique assessment program which efficiently addresses compliance and due-diligence requirements across multiple drivers (i.e. PCI, FFIEC, requirements from the state, federal laws, or other industry recognized best practices).

Advantages of AT&T

AT&T, through AT&T Cybersecurity Consulting and various acquisitions, has been delivering vulnerability assessments and penetration testing for more than 25 years. AT&T Cybersecurity Consulting performs hundreds of vulnerability assessments yearly and has conducted assessments for many similar organizations. AT&T currently delivers annual vulnerability testing and/or penetration test to the following.

- Ten of the fifty largest retailers
- One of the five largest pharmaceutical companies
- Several financial institutions

AT&T Cybersecurity Consulting's biggest differentiator is the ability to work with the entire AT&T organization on security issues. This allows AT&T Cybersecurity Consulting to work with the brightest people, including those in AT&T Managed Security Services (MSS), AT&T Chief Security Office (CSO) and AT&T Labs Research (Labs). AT&T Cybersecurity Consulting has access to all the innovation from AT&T as well. AT&T has always been an innovator and continues to be a leader in telecommunications and security. In the 1950s AT&T, through Bell Labs, was involved in early encryption projects and in the 1960s it was pioneering UNIX security controls. In the 1970s AT&T was involved with the development of the first vulnerability scanners and in the 1980s it was

advances in Internet Security Protocols. The 1990s brought the invention of the firewall and the ground breaking book, Firewalls and Internet Security, Repelling the Wily Hacker, written by AT&T employees William Cheswick and Steven Bellovin. In the last decade, AT&T has led in innovation such as the Network Based Firewall and other leading cloud related security offerings. In the future, look for additional cloud based security innovations and security around mobile devices, applications, and the Internet of Things (IoT).

AT&T Cybersecurity Consulting maintains a team of dedicated security practitioners who deliver on information security and regulatory compliance engagements on a daily basis. With customers across all market segments as well as federal, state, and local governments our team has been able to arrive at a hands-on understanding of the unique security challenges faced by these organizations.

Solution

The list of security services and assessment areas that DoIT has requested are listed in Table 1 below. While the requested services have been aligned with the established AT&T Cybersecurity Consulting Security Practice which would lead the fulfillment of the requested service, AT&T Cybersecurity Consulting will draw upon all of its security practice areas as needed to meet DoIT requirements. If selected as DoIT's security service provider, AT&T Cybersecurity Consulting will be responsible for the management of its resources as well as all vulnerability assessment activities associated with this program. These services will be provided in coordination with identified security program management team members within DoIT and in accordance with DoIT's policies.

Table 1. DoIT RFI Requirements Mapped to AT&T Cybersecurity Consulting Security Practice Areas

Vulnerability & Threat Management	Secure Infrastructure Services	Governance, Risk & Compliance
• External Network Vulnerability Penetration Testing • Internal Network Vulnerability Penetration Testing • Web Application / Database Penetration Testing • Physical Security Inspections and Testing • Wireless Network Penetration Testing	• VPN Configuration Reviews and Testing • Voice over IP Review and Testing • Trust Zone, DMZ & Network Architecture Testing / Reviews • Firewall and Router Configuration Reviews and Testing • Server Configuration Scanning / Reviews	• Information Security Risk Assessment Reviews • ISO, SANS, NIST FFIEC, and Other Compliance Security Assessments / Gap Analysis • Information Security Policy and Procedure Reviews • Security Awareness Program Reviews • Incident Response Program Reviews • Third Party Assessments

Vulnerability & Threat Management	Secure Infrastructure Services	Governance, Risk & Compliance
• Mobile / Android / IOS Application Security Testing • Virtual Infrastructure Security Penetration Testing • Social Engineering Testing • Software Source Code Reviews and Testing • Application Threat Modeling and Design Reviews • Secure SDLC Development Reviews • Revalidation Reviews	• Internal / External Trusted Cloud Assessments • Virtual Infrastructure Security Assessment • Revalidation Reviews	• Other assessments to determine compliance with State, Federal Laws, Regulations and Industry Recognized Standards • Revalidation Reviews

AT&T Cybersecurity Consulting will engage with the appropriate resources from DoIT to define requirements and scope for individual assessments. While each engagement will be tailored to the specific scope and objectives in question, at a high-level, AT&T Cybersecurity Consulting will follow the engagement model depicted in Figure 1 below.

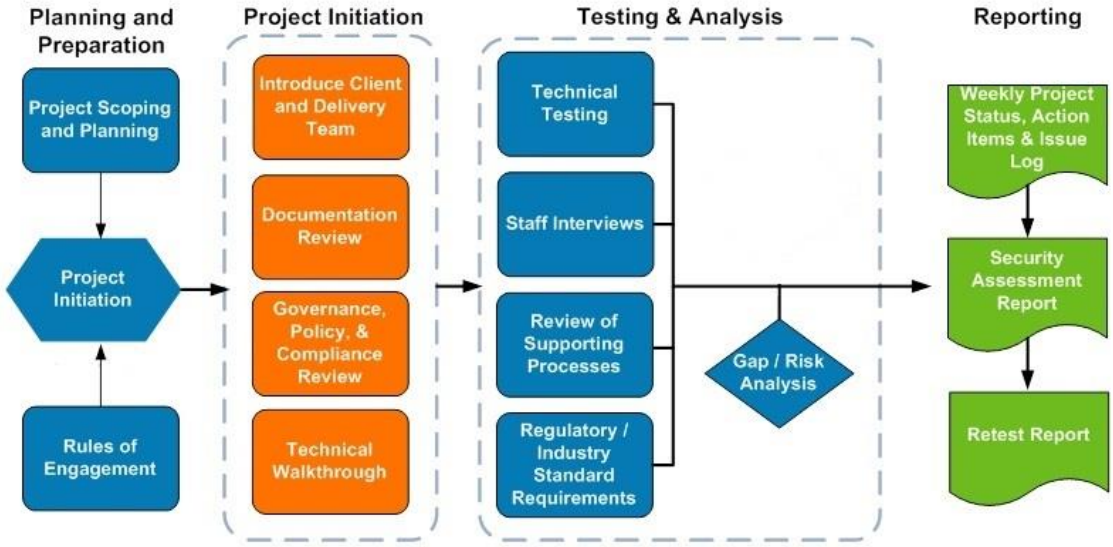


Figure 1. High-Level Engagement Flow

As one of the largest technology vendors of security services, AT&T actively participates with the rule makers and technology influencers in the medical and legal communities. AT&T maintains board seated members in the CSA (Cloud Security Alliance), ISA (Internet Security Alliance), and HIMSS operations, along with direct representation within the NCSL (National Committee of State Legislators).

Why AT&T?

Some of the key elements for DoIT to consider in evaluating the AT&T Cybersecurity Consulting response include:

- **Experience**—Strong history of delivering comprehensive and effective security, information risk, and compliance solutions to retail, healthcare, financial, and government.
- **Vendor Neutral**—AT&T Cybersecurity Consulting is not obligated to any security product vendors. Any suggestions for remediation actions or improvements in the DoIT security posture will be vendor neutral.
- **Trusted Advisor**—The regional consulting management team will manage the engagement and oversee the team. Delivery resources will be hand-selected to be part of the project team based on positive past experiences.
- **Broad Capability**—In addition to our security practice, AT&T Cybersecurity Consulting has extensive IT Strategy and Network Infrastructure skills in-house.

The measure of any successful security assessment is in the rigor applied to each task. AT&T Cybersecurity Consulting has built a rigorous solution set for conducting security assessments. Those solutions are based on the results of the collective body of knowledge that comes from performing these services for a variety of customers over an extended period of time. We look forward to demonstrating to DoIT how that knowledge can help them reach their information security, compliance, and operational objectives.

2. Scope

Based on the data provided in the Cybersecurity Assessment and the associated Q&A document(s), the following tasks were able to be identified and scoped. Additional services will be scoped jointly with DoIT on a go forward basis.

Activity	Scope
Ad-hoc Vulnerability Scanning	Description of Scope: Vulnerability scanning of in-scope network IP addresses both internally and externally. This includes access to a portal for reviewing scanning results.
External Network Penetration Test	Description of Scope: Internet based penetration against DoIT systems. Network Address Space in Scope: To be provided and/or confirmed by client in writing prior to testing.
Internal Network Penetration Test	Description of Scope: Penetration testing from within the DoIT network. Network Address Space in Scope: To be provided and/or confirmed by client in writing prior to testing. Geographic Locations: From within DoIT. Testing Dates: To be determined by AT&T Cybersecurity Consulting and DoIT Notes: - Include social engineering to drive penetration test success
Application Penetration Test	Description of Scope: Application penetration testing Internet-based and from within the DoIT network. Testing Dates: To be determined by AT&T Cybersecurity Consulting and DoIT
Device Configuration Assessment	Description of Scope: Security based review of select firewalls, routers, and other devices.
Network Architecture Assessment	Description of Scope: High level security-based review of the DoIT network architecture.
Wireless LAN Penetration Test	Description of Scope: Security assessment of 802.11 based DoIT networks.
Program, Policy, and Key Practice Review	Review of existing documentation related to information security including, but not limited to: • Information security strategic and tactical plans • Information security policy, supporting standards, guidelines, and procedures • Risk Assessment Methodology • Security Committee Charters • Security contractual clauses for outsourcing or other third-party relationships where the third party would have access to DoIT systems or information

Activity	Scope
	• Organizational charts of security department / program • Security-related Information Technology policies and procedures • Code of Conduct, Employee Handbook • Past assessments and audits • Network architecture documentation • Information security awareness and training materials • Business Continuity Plans • Software Development Lifecycle processes Interviews: Members of DoIT staff knowledgeable in information security, technology management, software development and technical administration.
Project Management	AT&T Cybersecurity Consulting will provide a project manager to plan and coordinate assessment activities between AT&T and DoIT.

3. Approach and Methodology

AT&T Cybersecurity Consulting will draw upon the following methodologies in delivering the requested services to DoIT. As requirements and engagements come to the fore, additional methodologies will be provide as required.

3.1 Network Penetration Testing Methodology

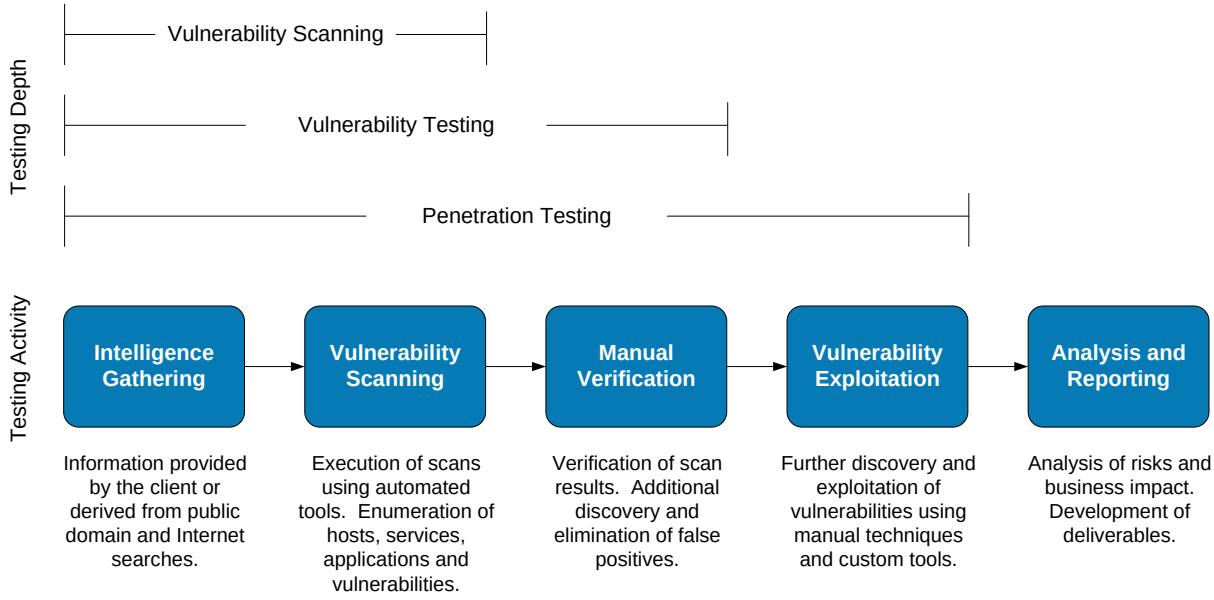
Objective

Vulnerability Testing determines the extent to which critical systems and sensitive information are vulnerable to compromise or attack. Penetration testing seeks to exploit the vulnerabilities identified in order to gain access to critical systems, sensitive information, or a specified trophy. This assessment will be conducted from the Internet, from an external perspective.

Methodology

AT&T Cybersecurity Consulting uses a combination of automated sweeps and detailed manual test steps to perform Vulnerability Testing. Information provided by the organization about the target environment will serve as an input for the automated scanning phase. AT&T Cybersecurity Consulting will review and manually validate the results of the scans and then will execute additional advanced tests to identify obscure vulnerabilities that the automated scans may have overlooked.

The figure below depicts the high-level approach AT&T Cybersecurity Consulting will use in order to meet the outlined objectives. AT&T Cybersecurity Consulting designed this service to progress from least intrusive to most intrusive, with each new phase building upon the intelligence gathered in the previous phase. This logical progression helps to ensure a thorough assessment of the targeted environment while improving AT&T Cybersecurity Consulting's ability to provide relevant, practical recommendations for improvement. The graphic identifies activities included in Vulnerability Assessments and Penetration Testing.



Prior to starting the assessment, AT&T Cybersecurity Consulting conducts a project initiation meeting where AT&T Cybersecurity Consulting and the client mutually establish the rules of engagement. These rules will establish the hours of testing, identify hosts specifically excluded from testing, and will generally guide the testing team in their efforts to perform a thorough test while minimizing business disruptions.

Intelligence Gathering

The objective of this first phase is to gain as much knowledge as possible about the target environment through a combination of non-intrusive and somewhat intrusive activities. Equipped with the results of these Intelligence Gathering activities, the team determines its execution plans for the subsequent phases.

- ***Project Based Information Gathering***—Based on our discussions with the key personnel, this assessment will consider information freely provided by the client to assist in the accurate identification of risks. As such, the first step in the Intelligence Gathering phase will be to obtain relevant technical documentation related to the target environment and to conduct informational meetings with appropriate staff so that AT&T Cybersecurity Consulting has the information necessary to provide accurate and efficient execution of this service.
- ***Public-domain Information Gathering***—This step is completely non-intrusive and involves identifying and profiling the network and systems through external inquiries and investigations using information that is freely available in the public domain.

- ***Network Mapping***—The Network Mapping step identifies specific network systems that AT&T Cybersecurity Consulting must traverse before reaching the target systems. AT&T Cybersecurity Consulting accomplishes this using both intrusive and non-intrusive techniques. In this regard, AT&T Cybersecurity Consulting frequently uses a "ping sweep" using Internet Control Message Protocol (ICMP), Simple Network Management Protocol (SNMP), and TCP "pings" to gather limited information about the target host. These sweeps will assist AT&T Cybersecurity Consulting in determining the full extent of systems and networks present and how they connect to untrusted networks. In most cases, AT&T Cybersecurity Consulting can use a combination of manual steps combined with tools such as hping, icmpush, nslookup, dig, and traceroute to facilitate this step.

Vulnerability Scanning

The objective of this phase is to identify hosts, services, and vulnerabilities in the target environment using a suite of customized tools. AT&T Cybersecurity Consulting performs two distinct steps during this phase: Host & Service Identification and Vulnerability Identification.

- ***Host & Service Identification***—AT&T Cybersecurity Consulting uses host and service identification activities to identify specific system and application information on targeted hosts and networks. AT&T Cybersecurity Consulting gathers information on features such as open ports, operating system types, software versions, available services, and the applications providing those services. AT&T Cybersecurity Consulting then uses this information to obtain lists of known or emerging vulnerabilities so the foundation for further testing can be established. This phase uses somewhat intrusive methods that may be detectable by properly installed and monitored intrusion detection systems.
- ***Vulnerability Identification***—After identifying all hosts, ports, and available services, AT&T Cybersecurity Consulting attempts to identify system and application vulnerabilities using a combination of commercial, open-source, and proprietary tools. AT&T Cybersecurity Consulting customizes some of these tools to improve the identification of advanced and emerging vulnerabilities. The result of the vulnerability identification step is an enumeration of possible vulnerabilities obtained through a combination of the various scanning and analysis tools.

Manual Verification

During this phase, AT&T Cybersecurity Consulting manually confirms the results from the automated tools. This activity serves to filter the data to improve the accuracy and

relevance of our technical findings report as it eliminates false positives yielded by the tools.

While the scans effectively identify a large portion of the vulnerabilities present, AT&T Cybersecurity Consulting also executes manual testing to identify certain complex, emerging, or obscure vulnerabilities. This phase does not generally include exploitation of the identified vulnerabilities to penetrate systems. However, 'inadvertent' exploitation may occur when the vulnerability, by its very nature, is exploited in the process of identifying its presence or when exploitation will identify additional and/or dependent vulnerabilities.

The activities AT&T Cybersecurity Consulting performs during this phase offer significant value over the sole use of automated tools. Often, these advanced techniques can be used to determine that vulnerabilities identified through automated tools only are false positives. Furthermore, such techniques allow AT&T Cybersecurity Consulting to identify previously undetected vulnerabilities as they can detect counter-security and attack techniques that obscure vulnerabilities from automated tools. For example, a common application running on a non-standard port may exhibit vulnerabilities not discovered by an automated scanner, but detectable using manual testing methods.

At the conclusion of this phase, AT&T Cybersecurity Consulting will enumerate and validate vulnerabilities discovered through both automated and manual means. Within the final deliverable report, AT&T Cybersecurity Consulting will note any particular vulnerability whose presence could neither be validated nor eliminated.

Vulnerability Exploitation

During this phase AT&T Cybersecurity Consulting will attempt to exploit some of the vulnerabilities identified and confirmed during the previous phases. AT&T Cybersecurity Consulting will execute exploits with the sole aim of fulfilling the specific goals of the penetration assessment; however, AT&T Cybersecurity Consulting will not actively exploit any vulnerability without obtaining permission from the client. Exploitation of certain vulnerabilities may lead to the identification of additional vulnerabilities that, in turn, may require further exploitation to identify potential problems. However, please note that AT&T Cybersecurity Consulting will follow this iterative process only to the extent necessary to accomplish the goals of the assessment.

AT&T Cybersecurity Consulting performs Vulnerability Exploitation using a variety of techniques, depending on the nature of the vulnerabilities. Attackers can exploit certain vulnerabilities by using a simple manual request, such as a directory listing on a web server, while others will require specially crafted commands or code. In some cases, AT&T Cybersecurity Consulting will use or modify open-source tools to accomplish this

task. Due to the nature of some vulnerabilities, AT&T Cybersecurity Consulting may not be successful in exploiting all vulnerabilities within the agreed timeframe for execution. In such cases, AT&T Cybersecurity Consulting will note this in the final deliverable report.

Analysis and Reporting

During the Analysis and Reporting phase, AT&T Cybersecurity Consulting analyzes the information gathered and documents the findings. AT&T Cybersecurity Consulting then assigns a rating to each risk identified, based on standards of good practice and AT&T Cybersecurity Consulting's extensive practical assessment experience.

Specifically, AT&T Cybersecurity Consulting categorizes the risk each finding poses to your enterprise as "High," "Medium," or "Low." AT&T Cybersecurity Consulting will also categorize the amount of effort required to implement each recommendation as "High," "Medium," or "Low".

3.2 Application Penetration Testing Methodology

Objective

AT&T Cybersecurity Consulting's Application Penetration Test determines the extent to which a particular application is vulnerable to an external attack. It examines the application for use of secure coding practices and identifies the risk exposure the application represents. AT&T Cybersecurity Consulting's execution of an Application Penetration Test uses a combination of automated testing practices and creative manual testing approaches. The automated portion of the assessment relies on automated tools to perform tasks such as spidering and identification of vulnerabilities which are easily detected from responses.

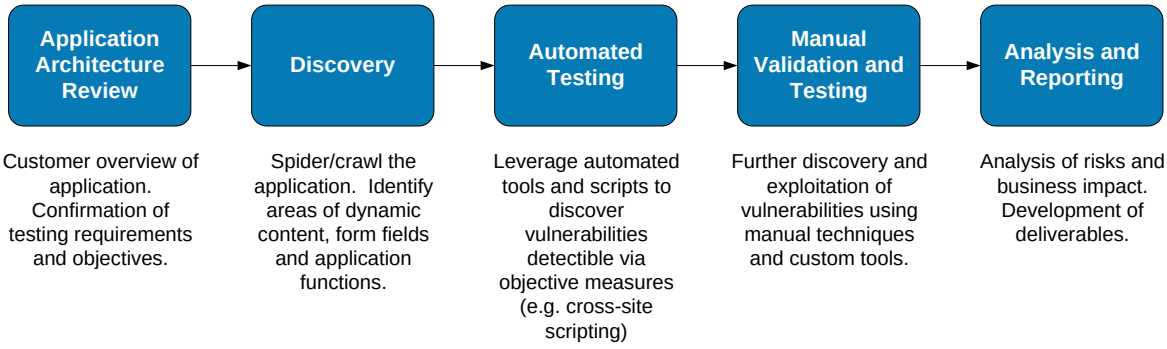
The artistry of the assessment service is based on the execution of numerous manual attacks. These are not easily automated and exploit the results from the automated assessment activities. Vulnerabilities are verified and placed in context using knowledge of the environment and prior experience with other clientele.

Methodology

AT&T Cybersecurity Consulting's Application Penetration Test service identifies security concerns of each application architecture component. AT&T Cybersecurity Consulting will begin the assessment by reviewing the application architecture with the development personnel, application administrator, or other applicable IT personnel, in order to gain an understanding of the application's use and administration. Network

diagrams of all hosts in question should be provided before the initial meeting so that AT&T Cybersecurity Consulting has a clear architectural representation of the application.

AT&T Cybersecurity Consulting follows a detailed approach to conducting web application testing, as described in the following sections. While this is primarily a manual test, AT&T Cybersecurity Consulting does employ some automated tools in assessing the application. AT&T Cybersecurity Consulting then analyzes the data and creates the technical findings report.



Application Architecture Review

This phase of the project begins with a meeting between the appropriate key personnel and the AT&T Cybersecurity Consulting Testing team. This meeting identifies the objectives of the application test and desired results. Following the initial objective identification, AT&T Cybersecurity Consulting and the Customer will perform a review of the application features and architectural components. The Customer will provide a diagram of functional components and other supporting documentation, if available, during this phase. This ensures that the team will quickly understand and focus their efforts on the specific objectives of the test. The Customer will also provide all URLs, and any user IDs and passwords required to access the application at this time.

Discovery

Upon the completion of the architecture review, AT&T Cybersecurity Consulting will begin the discovery phase of the assessment. This phase involves spidering or crawling the application to determine pages which exist, where dynamic content is likely being generated, and other preliminary data. This phase is generally automated; however, there are sites which spiders do not handle well, in which case the application is mapped via more manual techniques.

Results from the discovery tools are used to craft an attack plan. The attack plan focuses on areas that are often susceptible to web application vulnerabilities. Areas such as the authentication pages, form fields, and dynamically generated pages are marked for focus, while files such as images (i.e. .gif) and cascading style scripts (.css) are noted less important.

Automated Testing

Executing the plan of attack begins with the employment of automated tools and scripts. These tools provide value by testing a variety of attack vectors in a reduced time frame. Detection of potential cross site scripting, verbose errors and forceful browsing are aspects typically identified with automated tools. The other key result returned by automated testing is where the weakest portions of the application exist.

Manual Validation and Testing

During this phase AT&T Cybersecurity Consulting has two main objectives – to eliminate false positives from the previous phases and to exercise the features and functions provided by the application with the aim of escalating privileges and identifying potential vulnerabilities. AT&T Cybersecurity Consulting will attempt to escalate privileges both from the perspective of a valid user with a user ID provided by Customer or as a user without any assigned user ID (guest).

The following list provides potential vulnerabilities that are tested for, as they are the most likely to present the greatest risk to a web application environment. Actual testing may evaluate a number of additional types of issues.

- **Input Validation**—The majority of web application vulnerabilities are due to the lack of properly validating input. Common vulnerabilities associated with the lack of proper input validation include Command Injection attacks such as SQL Injection, cross-site scripting (XSS), Buffer Overflows and Form Manipulation.
- **Command Injection**—Using Command Injection, an attacker attempts to submit a special character to terminate the intended application function and cause the application to execute a command issued by the attacker. For example, in SQL injection, a single quote (‘) character is injected through an input field variable being used in a SQL query. The single quote character terminates the SQL statement normally built by the application and can allow an attacker to append additional query data to the statement. The application sends the query to the backend database, executing the attacker’s appended command. This type of attack can lead to a full compromise of the server by using internal database functionality.

- **Cross-site Scripting**—Cross-site Scripting attacks target a client web browser through the vulnerable web application. This form of attack utilizes the web application's lack of input validation to inject client-side code into the webpage. A common mistake in web applications is to pass error messages as part of the URL.
- **Buffer Overflows**—A buffer overflow is an anomalous condition where a program somehow writes data beyond the allocated end of a buffer in memory. Since program control data often resides in the memory areas adjacent to data buffers, a buffer overflow is used to execute arbitrary code and usually leads to a remote compromise of the server.
- **Form Manipulation**—Form Manipulation usually exists in web applications that attempt to hide information using "hidden" html form tags. Early on, a majority of these vulnerabilities resided in shopping cart programs that used this tag to hide the price of an item. This allowed an attacker to manipulate the price of an item. In this example, passing an item number via the form to a database and forcing the query to return the price for that item removes the problem.
- **Bypassing Access Controls**—In some cases, web developers have taken extra steps to implement filters into the application to handle input. However, it is possible to bypass these filters in some cases using a variety of techniques. It is common to find developers using client-side code, such as JavaScript, in forms via "onsubmit()" functions. Since JavaScript executes on the client side, an attacker can choose not to execute the code either by submitting variables directly via a URL or by saving the page locally and modifying the code.
- **Authentication and Authorization**—Authentication is the act of verifying a user's identity. Based on the identity, the application then authorizes the user to access various parts of the application. Improper account and session management as maintained by each application can allow unauthorized users elevated access to sensitive systems.
- **Account and Session Management**—Account and session management deals with all aspects of how a user manages their account, as well as how the application tracks active sessions. Account management may include mechanisms to remind a user of their password, change a password, or personalize their account information by uploading icons and adding signatures.
- **Error Handling and Information Leakage**—Error handling is the act of catching errors returned by applications and functions. In a web environment, this usually deals with HTTP errors such as error 404 and 500. Information leakage may occur through data returned in error messages or the source code of HTML documents. Developers should be careful to take into account what information

is viewable by users. AT&T Cybersecurity Consulting will attempt to obtain information by deliberately causing applications errors and evaluating the returned messages. These error messages could contain such things as directory structures, paths to sensitive server configuration files or database structures. In addition, comments in the code disclosing a developer's name and email address can assist an attacker with social engineering attempts.

- **Data Integrity and Confidentiality**—Proper data integrity and confidentiality implementation protects data from unauthorized modification and viewing. An attacker will normally try to compromise the data while in transit across the network but will be equally happy to compromise the data at the storage point. In a multi-tier web application environment, sensitive data traverses not only to and from a client, but also between tiers in the environment.

  In a web application environment, data stored in cookies, authentication processes and data stored in the HTML source are all areas of concern. Encrypting data in cookies, especially credential data, will help prevent tampering by the user.

  In many cases, developers implement base64 encoding to protect data instead of encryption. Using algorithms such as base64 to encode data provides little added security, as a simple web search provides numerous methods to decode base64 and reveal the hidden data. In addition, developers and Information Security should perform a comparative analysis of various types of encryption, and discard algorithms not adequate to protect the data.

- **Web Server and Application Configuration**—proper configuration of servers and applications can pose significant risks to a system's security. When web servers and third-party web applications ship, they often come with a number of default settings that are inherently insecure. In addition, a number of them include online documentation and interfaces installed by default. A high percentage of these have proven security flaws that usually allow an attacker to gain information about your environment or even remotely compromise the server.

Analysis and Reporting

During the Analysis and Reporting phase, AT&T Cybersecurity Consulting analyzes the information gathered and documents the findings. AT&T Cybersecurity Consulting then assigns a rating to each risk identified, based on standards of good practice and AT&T Cybersecurity Consulting's extensive practical assessment experience.

Specifically, AT&T Cybersecurity Consulting categorizes the risk each finding poses to your enterprise as "High," "Medium," or "Low." AT&T Cybersecurity Consulting will also

categorize the amount of effort required to implement each recommendation as "High," "Medium," or "Low".

3.3 Device Configuration Review Methodology

Objective

AT&T Cybersecurity Consulting performs device configuration assessments as part of a well-rounded Security Assessment. Proper device configuration is an important component of a defense in depth strategy for protecting information resources from internal and external attacks, and unauthorized access to sensitive information. The objective of a configuration review is to ensure that the proper controls are in place for critical devices, such as servers, firewalls, VPN gateways, network equipment and workstations.

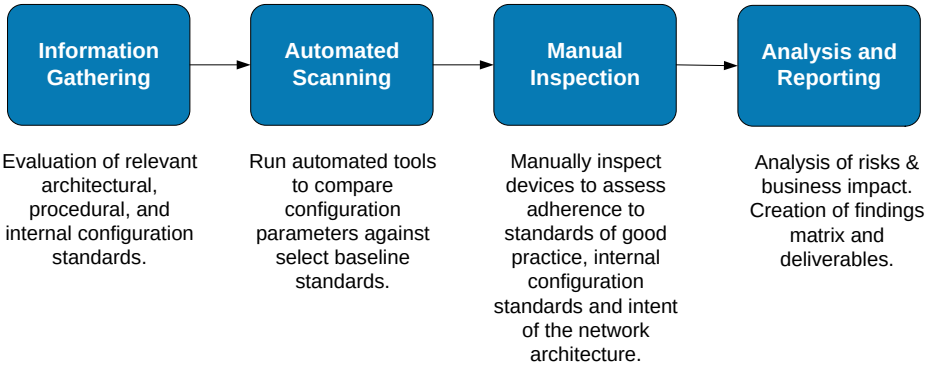
Methodology

For all devices assessed in the Configuration Review, AT&T Cybersecurity Consulting will focus on the following aspects of configuration:

- Vulnerable software version
- Proper access controls
- Proper remote access of the device itself (SSH, HTTPS, SSL/TLS, IPSec, etc.)
- Adequate and effective rules implemented
- Sufficient auditing and logging enabled on the devices
- Failover configuration (if implemented)
- SNMP configurations (if implemented)
- Efficient use of available security features

When reviewing these devices, AT&T Cybersecurity Consulting compares the current configuration against standards of good practice published by NIST, SANS, CIS, and AT&T Cybersecurity Consulting's own work in developing baseline hardening and system accreditation guides.

The following graphic depicts the workflow associated with the configuration reviews:



Information Gathering

During the first phase of the assessment, AT&T Cybersecurity Consulting will meet with the key personnel responsible for the organization's configuration policies and their implementation. These interviews will provide AT&T Cybersecurity Consulting with an opportunity to collect appropriate documentation related to the enterprise security policy and provide an overview of the current device configurations.

Automated Scanning

The objective of this phase is to gather information from the hardware and software regarding network information and configuration implementation using automated tools. These tools can include port and vulnerability scanners, as well as more specialized tools that target a particular service on the device, such as SMTP, SNMP, HTTP(S), etc.

Manual Inspection

During this phase, AT&T Cybersecurity Consulting manually confirms the results from the automated tools. This activity serves to filter the data to improve the accuracy and relevance of our technical findings report as it eliminates false positives yielded by the tools. In addition, AT&T Cybersecurity Consulting manually inspects the configuration information to identify any potential security risks.

Firewall Configuration Review: — The following criteria, specific to firewalls, will be assessed as part of the configuration review:

- Firewall design and approach
- Firewall management
- IP networking specifics
- Basic protection (anti-spoofing, denial of service)

- IP forwarding
- Source routing
- Firewall OS configuration
- Rule set configuration and definition
- Allowed inbound and outbound services
- Service proxies, circuit-level gateways, and packet filters
- Surrounding firewall security issues
- Access Control Lists

Windows Server & Workstation Configuration Review

AT&T Cybersecurity Consulting will assess the Windows systems baseline image and configuration standards by comparing the system configuration against standards of good practice. AT&T Cybersecurity Consulting compares the underlying OS against best practices for secure baseline configurations to determine where server configurations lack the necessary controls to achieve the maximum level of security while still supplying the required level of functionality. The following is an outline of the key areas AT&T Cybersecurity Consulting will assess:

- **Network Services**—Unneeded services and protocols are disabled including, Anonymous access to these services and remote-control services are secured or disabled.
- **Account Environment Settings**—Parameters such as password expiration and session timeouts configurations meet security needs.
- **Account Policy Settings**—Account policies for password rules, login time restrictions, user rights assignments, security options, and audit policies
- **Registry Settings and File System Protection**—User rights to registry and file system permissions are implemented according to best practices, and critical system files are protected.
- **Domain and Active Directory Settings**—Depending on the existing environment, permissions across a domain or active directory structure require stringent restrictions. This includes such things as file shares, GPOs, and other connection points.
- **Startup Files, Scripts, and Configuration Files**—Files executed at startup, run as batch procedures, or used as configuration parameters are configured with no special privileges and do not have the ability to escalate privileges.

- **Operating System Updates**—Application of the most recent and stable patches, including service packs, hot fixes, and critical fixes.
- **Encryption**—Determine that current encryption methods adequately protect the data, whether in transit or at rest. Compare algorithms and key length against suggested standards of good practice.

Unix/Linux Server Configuration Review

Similar to Windows Server configuration review, AT&T Cybersecurity Consulting will assess the UNIX systems baseline image and configuration standards by comparing the system configuration against standards of good practice. The following is an outline of the key areas AT&T Cybersecurity Consulting will assess:

- **Network Services**—Unneeded services and protocols are disabled. Remote control services are disabled, or secured with approved standard alternatives (ssh instead of telnet, etc.)
- **Account Environment Settings**—Parameters such as password expiration and session timeouts are configured to meet security needs.
- **Privileged Access Control**—Administrators use accounts separate from their normal account authentication and audit trail to perform system level functions.
- **Account Policy Settings**—Account policies for password complexity, login time restrictions, user rights assignments, security options, and audit policies.
- **Shared System Resources and Permissions**—Access to shared temporary storage file system and use of Set UID/Set GID on scripts or executable files.
- **Host Based Authentication (.rhosts & hosts.allow)**—Access to services and resources is not based upon remote hostname/address values.
- **Operating System Updates**—The most recent and stable patches are applied.
- **Encryption**—Determine that current encryption methods adequately protect the data, whether in transit or at rest. Compare algorithms and key length against suggested standards of good practice.

Analysis and Reporting

During the Analysis and Reporting phase, AT&T Cybersecurity Consulting analyzes the information gathered and documents the findings. AT&T Cybersecurity Consulting then assigns a rating to each risk identified, based on standards of good practice and AT&T Cybersecurity Consulting's extensive practical assessment experience.

Specifically, AT&T Cybersecurity Consulting categorizes the risk each finding poses to your enterprise as "High," "Medium," or "Low." AT&T Cybersecurity Consulting will also categorize the amount of effort required to implement each recommendation as "High," "Medium," or "Low".

3.4 Network Architecture Assessment Methodology

Objective

The purpose of a Network Architecture Review is to examine the overall network design to ensure it meets and incorporates industry standards and best practices. AT&T Cybersecurity Consulting will work with the network and security architects to get a complete understanding of the network environment and make relevant recommendations that allow security goals and objectives to be met. This review is not intended to be a comprehensive examination of each device on the entire network. Findings from this review will consist of recommendations for long-term enhancements to the networked environment including:

- Overall network design
- General perimeter controls
- Select topologies and network segments
- Third-party access

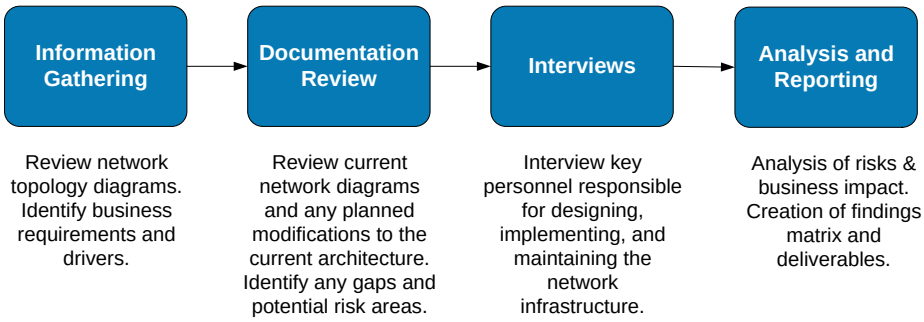
Methodology

AT&T Cybersecurity Consulting will conduct the network architecture assessment with the methodology outlined in this section. The following are likely elements of the network architecture that are within scope:

- Effective Network segmentation through use of the following:
  - DMZ configurations
  - Secure Enclaves
  - VLAN's
- Location of available services (VPN, RAS, proxies, etc.)
- Location of core current services
- Presence and configuration of firewalls and other filtering devices
- Wireless LAN infrastructure

- Planned architecture modifications and improvements
- Redundancy and Single Points of Failure
- Resilience to DoS/DDoS, Virus, and worm attacks
- Change Management
- Presence of specific technologies related to:
  - Anti-virus
  - Intrusion detection / prevention
  - Vulnerability and patch management
  - DDoS mitigation
  - Remote Access Solutions

The following figure depicts the workflow of an architecture assessment:



Information Gathering

During the first phase of the assessment, AT&T Cybersecurity Consulting will meet with the key personnel responsible for the organization's network architecture and maintenance. These high-level discussions will provide AT&T Cybersecurity Consulting with an opportunity to understand how the current architecture was developed, how it operates and the limitations with the current implementation.

Documentation Review

The next step in the assessment will be an evaluation of all relevant, available network documentation. This will allow AT&T Cybersecurity Consulting to understand the topology of the network, and the relevant design strategies employed in its architecture. Typical documents and diagrams that reviewed during this assessment include:

- WAN Topology

- LAN Topology
- Wireless Topology and hand-off points to wired infrastructure
- Network Architecture for Critical Business Applications
- Third Party Network Connections (customers, vendors, extranets)
- Remote Access Solutions
- Configuration Standards & Processes
- Change Management

Interviews

The next phase of the assessment consists of interviews with the staff responsible for maintaining and designing the architecture. These highly interactive sessions will involve discussions of the business drivers that led to the current architecture and their influence on future modifications.

Additional topics of discussion may be identified during the course of the review. Any potential security issues or outstanding configuration questions will be discussed with the key personnel.

Analysis and Reporting

During the Analysis and Reporting phase, AT&T Cybersecurity Consulting analyzes the information gathered and documents the findings. AT&T Cybersecurity Consulting then assigns a rating to each risk identified, based on standards of good practice and AT&T Cybersecurity Consulting's extensive practical assessment experience.

Specifically, AT&T Cybersecurity Consulting categorizes the risk each finding poses to your enterprise as "High," "Medium," or "Low." AT&T Cybersecurity Consulting will also categorize the amount of effort required to implement each recommendation as "High," "Medium," or "Low".

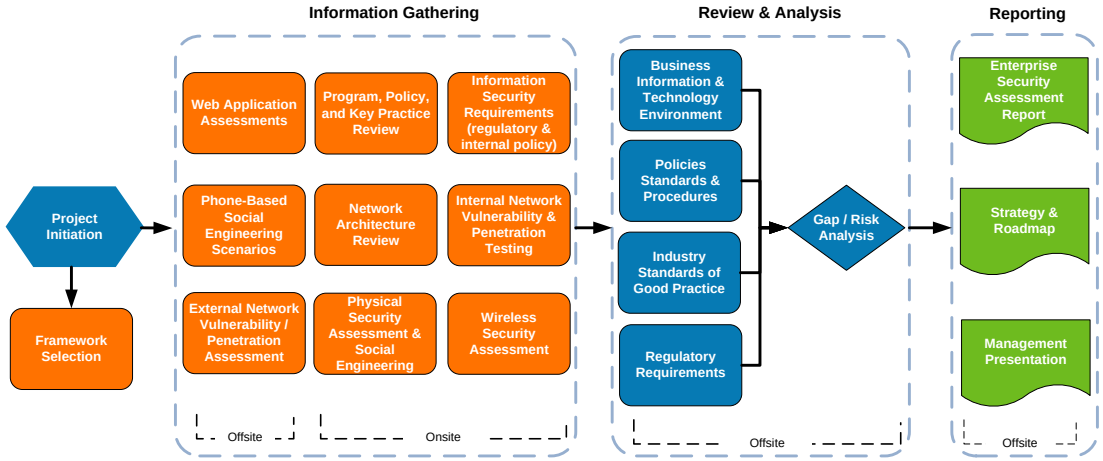
3.5 Enterprise Security Assessment Approach

Overall Approach

AT&T Cybersecurity Consulting's ESAs are designed to identify gaps in an organization's information security program using an established controls framework. The overall approach for the ESA is depicted below. Each assessment activity's approach and methodology are described within the subsequent sections.

- **Project Initiation Meeting and Project Management**—Ensure project expectations, project contacts, rules of engagement, etc. and develop detailed project plan.
- **Planning and Requirements Determination**—Determine and document requirements in which the Enterprise Security Program will be assessed against and customize assessment baseline.
- **Information Gathering**—Review documentation, departmental surveys, interview staff and suppliers responsible for aspects of information security, and perform testing activities
- **Review and Analysis**—Use information gathered to compare the security posture considering:
  - Defined standards of good practice—DoIT has requested NIST Cybersecurity Framework (CSF) as the basis for the analysis
  - Legal requirements for privacy and security
  - Common industry peer functions and practices
- **Reporting**—Develop recommendations and action plans to improve the Program from a Governance, Organization, Process, and Technology perspective.

The following figure depicts the overall project approach and steps.



Kick-Off Meeting and Project Initiation

AT&T Consulting recognizes the value of communication and ongoing collaboration with our customers. As such, we include a project initiation meeting (kick-off meeting) with all of our engagements. During the meeting, AT&T Consulting will do the following:

- Introduce key people from DoIT and AT&T Consulting Project Team
- Exchange contact information (for regular reporting and emergencies)
- Review scope of services
- Review communication, notification, and issue escalation procedures
- Discuss other specific DoIT requests and rules of engagement
- Discuss the involvement of the DoIT staff in the project for the purpose of knowledge transfer and security
- Discuss the deliverables required at completion of the project, the designated recipient, and the manner in which the AT&T Consulting Project Team will forward those deliverables

For the duration of the engagement, AT&T Consulting will provide day-to-day project management for all aspects of this project, including tracking and resolution of project related issues, progress tracking, project reporting, and communication. AT&T Consulting will assign a Project Manager/Lead to be the primary point of contact for all project management related issues.

A key component of AT&T Consulting's project management approach is timely reporting of project progress and findings. This enables a proactive approach to addressing security risks discovered during the course of the project and ensures that all project stakeholders are completely informed at all times. To support this, AT&T Consulting will issue regular status reports to [CLIENT'S] Project Sponsor/Manager. The frequency of these status reports is based on the project or client need and will be determined in the project kickoff meeting. Follow-up discussions will occur on a case-by-case basis to ensure clear and timely communication of all issues.

Requirements Determination and Framework Selection

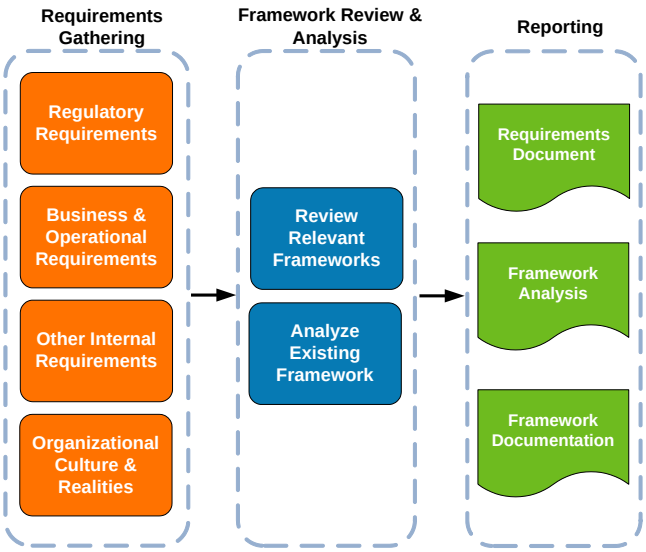
The first step is determination of the specific requirements that must be addressed by the information security program in the organization. In some cases, regulatory compliance, with government or industry regulations, is the primary driver; in other cases, specific enterprise risk management, business requirements, or corporate culture play a key role in the information security program. As such, AT&T Consulting will begin by understanding the overall mission of the organization, its organizational structure, corporate culture, key business and operational processes, and existing IT environment. We will gather information by meeting with business, administrative, and technology staff, both at management and technical levels. A review of existing documentation, such as strategy documents, code of conduct, key business and operational processes

workflows, enterprise risk management mandates, and any (documented) needs specific for the organization.

Once AT&T Consulting has an adequate understanding of requirements for the information security program, along with likely priorities, we will examine the framework on which the existing program is built-upon. AT&T Consulting will analyze both the existing framework, if any, and other relevant, industry-recognized frameworks in the context of the requirements gathered in the previous step. If a framework had not been previously selected by the client an analysis of the requirements of relevant frameworks, along with a recommendation for selecting a framework for the information security program will be provided to the client. If a framework had already been chosen by the client, AT&T Consulting will provide an analysis of how well the framework addresses the requirements gathered and rationale for changing frameworks, if necessary or appropriate.

AT&T Consulting will facilitate internal meetings with business, administrative, and technology staff to discuss the proposed framework, collect feedback, and assess the potential impact to various areas in the organization. Furthermore, AT&T Consulting can assist the client with efforts to obtain buy-in and consensus from internal groups for the selected information security framework.

The outcome of the requirements gathering is a prioritized list of requirements for information security program and a recommendation for an information security framework, either new, re-affirm existing selection, or an alternate selection than the current selection. The overall Needs Analysis/Framework Establishment Methodology process is documented below:



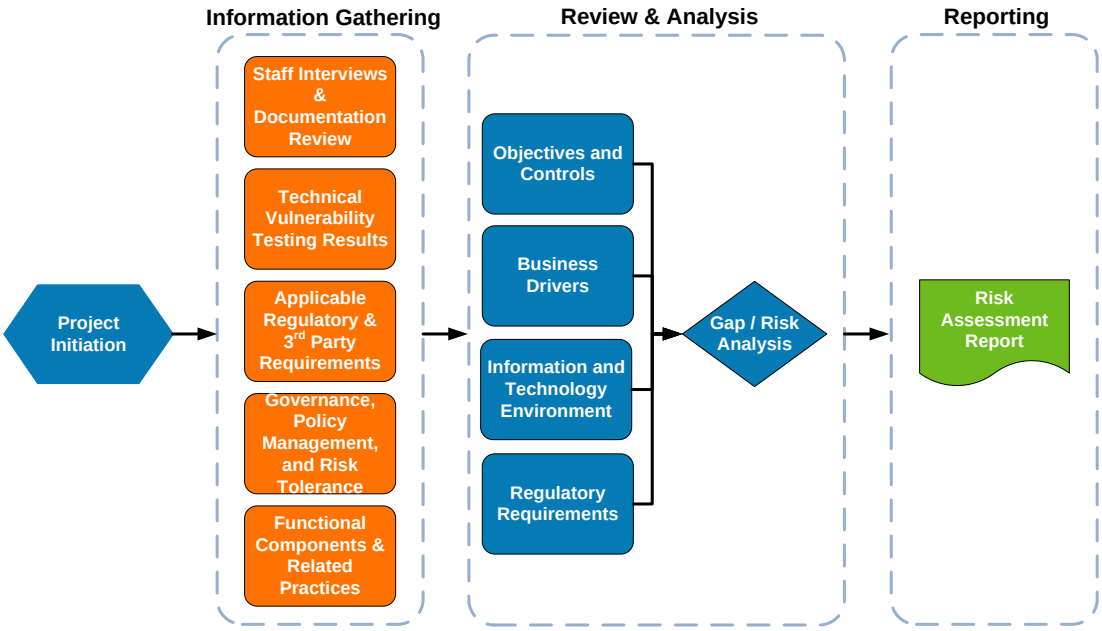
3.6 Cybersecurity Risk Assessment

Approach Overview

AT&T Cybersecurity Consulting's methodology to conducting the Information Security Risk Assessment includes project initiation, assessment approach, and any remediation follow-up. Each of these project phases is clearly defined below. At the conclusion of this project, DoIT will be provided a Risk Assessment Report, which will identify any findings and recommendations to assist DoIT in reaching compliance with the specified requirements. AT&T's methodology for assessing risk is based on NIST 800-30 rev 1. It is important to note that AT&T Cybersecurity Consulting does not offer any opinions of legal compliance. The following figure provides a visual sample of the AT&T Cybersecurity Consulting assessment process.

The following figure depicts the overall project approach and steps.

Figure 2: Engagement Process Flow



Project Overview

In addition to the project initiation meeting, AT&T will utilize the approach summarized below, to meet project objectives:

- **Information Gathering**—Review documentation, survey results from the ESA, and interview DoIT staff; collect evidence on process implementation

- **Review and Analysis**—Based on the survey results, categorize state entities according to the scope of the risk. Use information gathered to compare DoIT's Information Security Program Structure, Practices, Policies and Procedures to the standards of good practice, namely the NIST Cybersecurity Framework (CSF).
- **Reporting**—Develop prioritized recommendations to correct identified deficiencies, weaknesses, and gaps in DoIT's information security program, policies, procedures, and controls. The report will:
  - Identify and categorize state entities according to existing IT security controls, network vulnerability gaps, and other factors by risk category
  - Identify and categorize state entities according to existing defense and incident response policies, procedures, disaster recovery plans, etc., by risk category
  - List findings and recommendations for IT threat mitigation
  - Apply risk assessment findings to create a Plan of Actions and Milestones (POAM)
  - Provide detailed remediation guidance recommendations
  - Provide post-assessment guidance

Information Gathering

During this engagement, AT&T will collect all relevant information through documentation reviews, survey results, and staff interviews with DoIT's staff. Staff interviews provide a forum to ensure that business drivers and key risk areas are fully considered during the assessment. This project will include a combination of onsite and remote work. Onsite work is conducted early during the engagement during which time AT&T focuses on information gathering to gain a better understanding of DoIT's Information Security Program management practices, Policies and Procedural implementation, and the environment including:

- Identification of DoIT's Information Security organizational structure and key stakeholders within this structure with roles and responsibilities affecting DoIT's Information Security Program Structure, Practices, Policies and Procedures.
  - The Information Risk environment.
- DoIT's efforts to perform effective Risk Analysis and Risk Management.
  - Governance, Policy Management, Acceptable risk tolerance.
  - Steering Committees and Working Groups focused on information security.
  - Privacy officials and other individuals designated by the covered entity with the responsibility of developing and implementing privacy policies and procedures as well as receiving privacy-related complaints.

  - Information security planning activities, such as communication of policies to all employees in the organization.
  - Additional functional components of the security program and the key practices supporting the program components.
  - Existing and planned initiatives affecting information protection within the DoIT environment, such as process initiatives (ITIL, quality management, process re-engineering, etc.), major technology implementations, organizational restructuring.
- Critical issues confronting DoIT.
  - The general technical architecture.

As stated above, AT&T will derive most of the information necessary to assess the environment and supporting key practices through documentation reviews, such as policies, procedures, and plans related to information security, and interviews and subsequent discussions with knowledgeable staff responsible for various aspects of Information Security Management. These may include:

- Executive Management
- Key business unit leaders
- Information Security Leadership and staff
- Staff in charge of both, Policy approval and Review
- Staff focused on Privacy
- Steering Groups and Committees
- CIO / IT Management / Administrators / Developers
- Staff focused on Business Continuity and Disaster Recovery
- Support Functions (HR, Legal, Facilities)
- Established committees and working groups
- Others, as applicable

<u>Review and Analysis</u>

During remote work activities, AT&T professionals will analyze the information gleaned from information gathered during the previous step. The objective is to identify critical issues and develop prioritized recommendations for improvement. AT&T will review and evaluate DoIT's security posture against the following:

NIST 800-53

From a program perspective, AT&T will identify committees and working groups focused on Information Security supporting and guiding compliance efforts with NIST 800-53 rev 4 (Security and Privacy Controls for Federal Information Systems and Organizations), the aim of which is to review the effectiveness of these functions and the roles within along with a higher-level review of DoIT's overall Information Security organization structure. Information gathering activities at the program level are aimed at understanding the roles and responsibilities within such functions, levels of management commitment, related axioms and objectives, evidence of activities and follow up, communication lines and links between those interpreting Information Security requirements and those responsible for implementing and maintaining controls to comply with these requirements.

This assessment will focus on the requirements for specific Policies, Procedures and Standards relating to the following NIST 800-53:

- **Access Control**—This categorization of standards requires that access to information, information assets, and business processes is based upon business and security requirements. Controls include: Authorized Access to Information Systems; Network Access Control; Operating System Access Control; and Application and Information Access Control
- **Communications and Operations Management**—This categorization of standards requires that operating procedures shall be documented, maintained and made available to all users who need them. Controls include: Documented Operating Procedures; Control Third Party Service Delivery; System Planning and Acceptance; and Monitoring
- **Information Systems Acquisition, Development and Maintenance**—This categorization of standards covers business and security requirements for new information systems (developed or purchased), or enhancements to existing information systems. Controls include: Correct Processing in Applications; Security of System Files

The table below lists the main components of the assessment and how they fit into AT&T Cybersecurity Consulting's approach to addressing security from a people, process and technology perspective.

Component / Element	Description
Oversight and Governance	
Strategy	Strategy development, alignment to business strategy and objectives, business Involvement in program, security involvement in business decisions

Component / Element	Description
Governance and program management	Governance bodies and decision structures, resource management, budgeting, benchmarking, security metrics and performance management
Risk management	Risk context, risk identification, risk analysis, risk evaluation, risk treatment (remediation, transfer, acceptance processes, risk tracking, and risk reporting)
Compliance management	Compliance research and identification, Policy management lifecycle (creation, approval, distribution, maintenance, exceptions), control framework management, control testing, compliance reporting, privacy management
Audit and Assurance	Security alignment with internal audit; external, independent review of security policies and programs, audit response management, response to third-party assessments
People	
Security services	Security service catalog and SLAs and service request response management
Security training and awareness	Security branding and marketing, security training, awareness, and behavioral change, security awareness and behavior measurement, and security in employee performance metrics
Security organization	Staffing, organizational structure and reporting, security staff training and certification, and security staff knowledge and experience
Business relationship	Commitment from executives and business leaders, business and customer engagement, knowledge transfer to business and executives, Relationship with relevant corporate functions
Roles/responsibilities	Security responsibilities for IT staff, corporate security, third-party partners, business users
Process	
Access Control	Access management including requesting, approving, modifying, and terminating access, privileged access management, remote access.
Threat and vulnerability management	• Threat intelligence: Threat intelligence program, collection and processing, analysis, production, and dissemination • Vulnerability management (including scanning, remediation, and threat modelling), configuration management, and patch management
Investigations and records management	• Log retention, records retention • Forensic services, including endpoint forensic capabilities
Incident management	Incident response preparation and testing, incident detection and analysis, incident containment, eradication, and recovery, post-incident review, and improvement

Component / Element	Description
Third-party risk management	Third-party risk management strategy and program, sourcing / IT procurement involvement, third-party security assessments (initial and ongoing), contract management, third-party personnel assessments, exit strategies
Information asset management	Asset ownership, asset classification, asset inventory and protection of assets throughout the lifecycle
Application/systems development	Review the SDLC and ensure security is incorporated.
Business continuity and disaster recovery (BC/DR)	Business impact analysis and risk assessment, contingency planning, business continuity plan (BCP) development, BCP training, BCP testing, BCP maintenance.
Technology	
Network	Intrusion protection, remote access, network segmentation and perimeter control gateways, network vulnerability management, network analysis and visibility, dynamic malware analysis, and DDoS protection
Databases	Database encryption, database monitoring, database configuration management, database vulnerability assessment, database masking
Systems	Storage security, configuration management, system hardening and protection, server antimalware
Endpoints	DoIT encryption, strong authentication, endpoint malware protection, endpoint configuration management, endpoint application control, host firewall/IPS, mobile security and device management
Application infrastructure	Secure network gateway, authentication and authorization, application firewall, application vulnerability management, static/dynamic application security
Messaging, content, and social media	Message encryption, web content filtering, social media risk and compliance, anti-malware, content filtering (e.g., antispam)
Data	Enterprise encryption and key management, digital/enterprise rights management, secure file transfer, file sharing, and collaboration, data leak protection (DLP)

As stated above, AT&T Cybersecurity Consulting will derive most of the information necessary to assess the environment and supporting key practices through documentation reviews, such as policies, procedures, and plans related to information security, surveys of users of the State's network, and interviews and subsequent discussions with knowledgeable staff responsible for various aspects of information security management. These may include:

- Executive Management

- Key business unit leaders
- Information Security staff
- Staff focused on Privacy
- CIO / IT Management / Administrators / Developers
- Support Functions (Legal)

Review and Analysis

During offsite work activities, AT&T Cybersecurity Consulting professionals will analyze the information gleaned from documents provided and interviews with various DoIT staff. The objective is to:

- Understand roles and responsibilities associated with the establishment, implementation, and management of the security at each of the subsidiaries
- Identify gaps and associated risks as compared to the assessment baseline and requirements identified
- Assess the maturity of the subsidiaries processes and technology
- Develop prioritized recommendations and actions plans to improve and transform the Program

Risk Analysis

The objective of this phase is to analyze the data gathered and determine factors that influence risk for the environment. Risk is a function of the likelihood of a given threat exploiting a potential vulnerability and the resulting impact of that adverse event upon the organization. This phase seeks to determine all of these potential inputs into the risk equation and determine the final risk for a particular element.

The risk equation involves several distinct parts, presented below:

- Control Analysis / Assess Security Measures
- Likelihood Determination
- Impact Analysis
- Risk Determination

The objective of **Control Analysis** is to analyze the controls that have been implemented and how they minimize or eliminate the likelihood of a threat exploiting a vulnerability. A control may mitigate a vulnerability itself or minimize the ability of a threat to reach that vulnerability. Security controls encompass both technical and non-technical controls, and the methodology also accounts for the layering of controls in a Defense-in-Depth strategy. Controls may be preventative or detective, and each may have several different effects on different vulnerabilities. Finally, some controls may require additional controls to be in place to be effective (for example, a detective control is only good if there is a procedure to have someone review the control's outputs on a periodic basis – if the alarm goes off and nobody is paying attention, is the alarm actually doing any good?).

The **Likelihood Determination** considers the threat-source motivation and capability, the nature of the vulnerability, and the existence and effectiveness of current controls. The combination of these factors indicates the probability that a potential vulnerability may be exploited within the context of the associated threat environment.

The **Impact Analysis** measures the adverse impact that results from a successful breach (a threat is able to exploit a vulnerability). The impact does not gauge any likelihood or ability of the threat to exploit the vulnerability, but rather seeks to detail what *would* happen *if* a breach was successful. There may be several impacts, from system down time to financial losses from espionage, and may be tangible or intangible. The adverse impact is typically characterized in one or more of the three areas of information security: loss of integrity, loss of availability, or loss of confidentiality. Measures of impact will typically be qualitative instead of quantitative, as qualitative impacts are better suited to prioritization.

All of the analyzed information is used to arrive at the **Risk Determinations**. This step assesses the risk to the business within the in-scope environment. The overall risk represents the likelihood of a given threat-source attempting to exploit a given vulnerability, the magnitude of the adverse impact that would occur if the exploitation were to be successful, and the adequacy of security controls in reducing or eliminating the risks in some way. As mentioned, AT&T Cybersecurity Consulting will address factors around people, process, and technology risk:

- Business factors such as organizational risk, partnerships risk, or revenue risk
- Technology factors such as network/systems design, security controls, proactive monitoring
- People and Process factors such as policies and guidelines, training efforts

DoIT knows its business, environment, and risk tolerance best, and as such it is important to evaluate and measure risks in a collaborative manner. AT&T Cybersecurity Consulting will, based upon experience, and the information gathered and analyzed will recommend a risk rating and discuss the conclusion with DoIT.

The risk levels are determined through a matrix incorporating the likelihood and impact (example below) based on NIST 800-30 rev 1. The values for the likelihood and impact are multiplied and the final score determines the risk based on the risk scale. The values and scales are arbitrary in these examples but show how a final risk calculation is achieved.

Table 1: Risk Determination Matrix

Threat Likelihood	Impact				
	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Very High (5)	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
High (4)	Very Low (1)	Low (2)	Moderate (3)	High (4)	Very High (5)
Moderate (3)	Very Low (1)	Low (2)	Moderate (3)	Moderate (3)	High (4)
Low (2)	Very Low (1)	Low (2)	Low (2)	Low (2)	Moderate (3)
Very Low (1)	Very Low (1)	Low (2)	Very Low (1)	Low (2)	Low (2)

Maturity Ratings

In addition to providing a narrative summary of our findings related to program maturity, AT&T Cybersecurity Consulting will assign a relative maturity rating to each so that DoIT can gain a better understanding of their overall posture. The maturity assessment will be organized around the content of DoIT's Program to be assessed. Based upon the results of information gathering, AT&T Cybersecurity Consulting will then rate and AT&T Cybersecurity Consulting will uses ratings based on maturity models commonly used within industry (e.g., Carnegie Mellon University's Capability Maturity Model or the Program Review for Information Security Management Assistance (PRISMA) maturity levels) and will customize the scorecard to align with DoIT's Program functions.

Table 1: Process Maturity

Level	Process Capability / Maturity	
1	1.	Incomplete or non-existent
2	2.	Ad hoc, sporadic implementation
3	3.	Formalized, but inconsistently accepted and implemented
4	4.	Universally accepted, quantitatively managed
5	5.	Optimized

While this numerical scoring model is based on a subjective evaluation of a particular process or control and consequently subject to minor inconsistencies and inaccuracies, it does provide a useful gauge of process capability and can be used to focus actions and priorities, as well as benchmark the program going forward.

Cybersecurity Risk Assessment Report Development

Cybersecurity Risk Assessment Report

AT&T Cybersecurity Consulting will develop prioritized recommendations (categorized by state entity), aligned with the maturity of the Program functions, to improve information security practices. The recommendations to improve the environment will be based on compliance requirements, industry standards, business requirements, internal security-related requirements, and practices used by industry peers. This will incorporate findings from the Network Architecture Review and Security Tools Review.

As part of this activity, AT&T Cybersecurity Consulting will ensure that our recommendations and supporting rationale are clearly understood, actionable, and appropriate for the environment. AT&T Cybersecurity Consulting will present any documentation detailing our findings and recommendations in a draft form to provide with an opportunity to review, comment, correct, and approve the format and content prior to finalizing the deliverable documentation. This iterative process helps to ensure that DoIT can make informed, incremental decisions regarding specific courses of action throughout this review.

3.7 Program, Policy, and Key Process Review

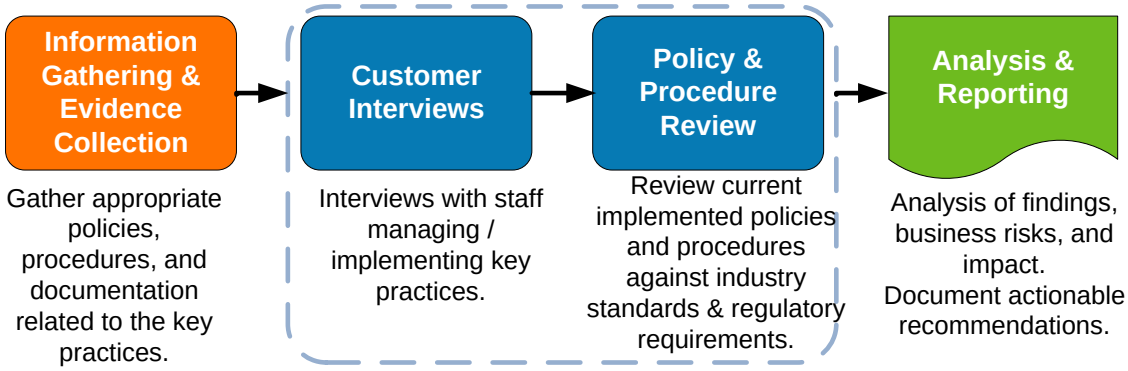
Objective

AT&T Cybersecurity Consulting's Program, Policy and Practice Review is designed to:

- Analyze the organization's existing information security program, related policies, processes, and practices to well-accepted industry standards, practices and regulatory requirements, where applicable
- Assess the reasonableness and effectiveness of existing information security controls given the organization's business objectives and associated risk/threat profile
- Identify any gaps from standards of good practice, and identify the need to complete and/or expand existing controls
- Cross reference and interlink findings with technical activity conducted as a part of this engagement or past assessments
- Provide recommendations to improve the organization's security posture and meet the desired end state based upon risk tolerance and compliance needs

Methodology

AT&T Cybersecurity Consulting will conduct a review of the governance structure, overall program foundation, and key practices considered essential for maintaining an appropriate information security and privacy posture. The following diagram provides an overview of our Program, Policy, and Key Practice Review.



Information Gathering

AT&T Cybersecurity Consulting will collect all relevant information through documentation reviews and staff interviews and verify gathered data. This project will include a combination of onsite and remote work. AT&T Cybersecurity Consulting conducts onsite work early during the engagement. During this time, AT&T Cybersecurity Consulting focuses on information gathering to gain a better understanding of the information security program, policy and procedural implementation, and the environment including, but not limited to:

- Identification of the organizational structure and key stakeholders in security management activities
- The information risk environment
- Governance, policy management, acceptable risk tolerance
- Information security planning activities
- Additional functional components of the security program and the key practices supporting the program components
- Existing and planned initiatives affecting information protection within the DoIT environment, such as process initiatives (ITIL, quality management, process re-engineering, etc.), major technology implementations, organizational restructuring
- Operational risk and compliance activities
- Critical issues confronting DoIT
- Prior information security-related assessments
- Specific practices surrounding:
  - Security program and governance
  - Policy management (security policies, procedures, and standards)
  - Information Risk Management
  - Physical security (including a tour)
  - Physical security controls pertaining to electronic forms of data and intellectual property
  - Human Resources Security
  - Security awareness and training
  - Operational security including configuration and patch management, vulnerability detection and management, network controls, network authentication, and antivirus and malware protection
  - Auditing and monitoring covering log analysis, host-based IDS, network IDS and Intrusion prevention systems (IPS), security information event management, and event correlation
  - Outsourcing and third-party controls
  - Security within the Systems Development Life Cycle (SDLC)
  - Business Continuity and Disaster Recovery Planning and testing
  - Information Security Incident Management

- Access controls security and strong authentication for internal and external (remote) access
- Compliance with laws and regulations

As stated above, AT&T Cybersecurity Consulting will derive most of the information necessary to assess the environment and supporting key practices through documentation reviews, such as policies, procedures, and plans related to information security, and interviews and subsequent discussions with knowledgeable staff responsible for various aspects of information security management. These may include:

- Executive Management
- Key business unit leaders
- Information Security staff
- Staff focused on Privacy
- CIO / IT Management / Administrators / Developers
- Staff focused on Business Continuity and Disaster Recovery
- Support Functions (HR, Legal, Facilities)
- Others, as applicable

Review and Analysis

During remote work activities, AT&T Cybersecurity Consulting professionals will analyze the information gleaned from documents provided and our interviews with various staff. The objective is to identify critical issues and develop prioritized recommendations for improvement. AT&T Cybersecurity Consulting will assess the current environment and security management practices against industry standards by conducting a gap and risk analysis of current practices against that baseline.

AT&T Cybersecurity Consulting will then determine the ability of existing practices and safeguards in meeting compliance and industry standards, business requirements, and identify DoIT risk tolerance. Where controls are not fully implemented within the DoIT environment, AT&T Cybersecurity Consulting will provide prioritized recommendations, based upon risk, so that DoIT can meet the requirements and strengthen its overall security program.

Reporting

Using the results from the previous steps, AT&T Cybersecurity Consulting will develop prioritized recommendations to improve DoIT information security practices. The recommendations to improve the environment will be based on compliance requirements, industry standards, business requirements, internal security-related requirements, and practices used by industry peers.

As part of this activity, AT&T Cybersecurity Consulting will ensure that our recommendations and supporting rationale are clearly understood, actionable, and appropriate for DoIT environment. AT&T Cybersecurity Consulting will focus on the key practices identified by DoIT. AT&T Cybersecurity Consulting will present any documentation detailing our findings and recommendations in a draft form to provide DoIT with an opportunity to review, comment, correct, and approve the format and content prior to finalizing the deliverable documentation. This iterative process helps to ensure that DoIT can make informed, incremental decisions regarding specific courses of action throughout this review.

4. Project Deliverables

AT&T Cybersecurity Consulting will provide the following deliverables as part of this project:

Name of Deliverable	Description of Deliverable
Assessment Reports	For each assessment, a final report covering the in-scope activities will be provided. The report will contain the following sections: • **Executive Summary**: — A high-level description of the activities performed by AT&T Cybersecurity Consulting and a summary of the pertinent findings. The executive summary is written in non-technical language to ensure a broad understanding of information security shortcomings, impacts and recommended actions, suitable for senior management consumption. • **Approach:** — High level discussion of the objectives and a description of the tasks performed by AT&T Cybersecurity Consulting. • **Summary Findings**: — A synopsis of the findings in the assessment targeting on central themes. • **Detailed Findings**: — A comprehensive list of findings that encompass each of the assessment components including a detailed discussion that explains the vulnerabilities discovered by AT&T Cybersecurity Consulting and a set of recommendations to address each finding. • **Appendices:** — Supporting documentation to substantiate and help recreate the finding after the assessment.
Final Report	A final report providing a compilation of all controls, findings, gaps and areas for improvement will be provided. This report will use the NIST Cybersecurity Framework to organize the content.
Project Plan	A detailed project plan will be provided during the initial phases of the engagement. It will be revised during the course of the assessment as modifications to engagement activities are identified. A final plan will be provided showing the completed tasks against planned tasks.

The findings in the assessment reports will be provided in a matrix format, similar to the example on the following page.

	Finding Description	Affected Systems	Overall Risk Level	Exploit Impact	Exploit Likelihood	Effort to Remediate	Remediation Suggestion
	Spoofed Email The remote hosts are running a mail (SMTP) server on TCP port 25. It is possible to telnet to this port and send a spoofed email message with the sender's email address matching internal company email addresses. AT&T Cybersecurity Consulting successfully sent a spoofed email message from one of these servers.	10.10.22.47 10.10.22.48 192.168.1.12 192.168.1.35	High	Medium	High	Low	Upgrade send mail to the most recent version. Versions above 8.9 have relaying disabled by default. If upgrading is not possible, configure the mail service to perform "Mail From" verification • Please see http://www.sendmail.org/tips/relaying for more information To prevent mail relaying on Exchange systems, please see http://technet.microsoft.com/en-us/library/dd277329.aspx
	Microsoft Windows Graphics Device Interface Integer (GDI) Overflow Vulnerability A vulnerability exists in the way GDI handles integer math. An integer overflow could occur while calculating the	10.10.22.47 10.20.30.45 192.168.1.1 192.168.1.5	High	High	Medium	Low	Microsoft has released a patch, which is available at http://www.microsoft.com/technet/security/Bulletin/ms08-071.mspx. If the patch cannot be installed, consider disabling metafile processing by modifying the registry.

	Finding Description	Affected Systems	Overall Risk Level	Exploit Impact	Exploit Likelihood	Effort to Remediate	Remediation Suggestion
	buffer length, which results in an undersized heap buffer being allocated. This buffer is then overflowed with data from the input image file. This could allow an attacker to execute arbitrary code with the privileges of the current user.						HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize create a DWORD entry "DisableMetaFiles" and set the value to 1. • Further details of this vulnerability can be found at http://labs.idefense.com/intelligence/vulnerabilities/display.php?id=762

Findings in the aforementioned matrix are prioritized based on overall risk level. The table on the following page explains what each column details and what the correlated risk rating indicates.

Finding Description	**This column provides a brief technical description of the finding in question. More detailed information or issue-related screenshots will typically be provided in a subsequent section or appendix, if necessary.**
Affected Systems	**This column lists the IP Address, hostname or a description of the system vulnerable.**
Overall Risk Level	**This section indicates the overall risk to a system that a given finding implies. This is typically a subjective analysis of the exploit difficulty in conjunction with the exploit impact. A rating of high, medium, or low will be suggested as follows:** **High** – The system is susceptible to a high level of risk. The issue should be addressed as quickly as possible. **Medium** – The system is susceptible to significant level of risk. The issue should be incorporated into the system development life-cycle and addressed in due time. **Low** – The system is mildly susceptible to exploit. The issue should be addressed based on resource and business impact considerations.
Exploit Impact	**This section indicates the impact a given finding has on a system when exploited. A rating of high, medium, or low will be suggested as follows:** **High** – The finding may result in a serious compromise of the system in question. This may imply an actual shell-level compromise (i.e. root or administrator) or a significant compromise of confidential information assets (i.e. database mining). **Medium** – The finding may result in a significant compromise of the system in question. This may imply the theft of a user-credential, or the ability to access limited information assets on the system. **Low** – The finding may result in a relatively mild compromise of the system in question. This may imply minor information disclosure or common misconfiguration issues.

Exploit Likelihood	**This section indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment and depends on the threat-source motivation and capability, the nature of the vulnerability, as well as the existence and effectiveness of current controls. A rating of high, medium, or low will be suggested as follows:** **High** – The attacker is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective. **Medium** – The attacker is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability. **Low** – The attacker lacks motivation or capability, or controls are in place to significantly impede, if not prevent, the vulnerability from being exercised.
Effort To Remediate	**This column indicates the required effort necessary for issue remediation. A rating of high, medium, or low will be suggested as follows:** **High –** There will be highly significant remediation and development effort required measurable in a quantity of days to weeks. **Medium –** There will be significant remediation and development effort required measurable in a quantity of hours to days. **Low** – There will be little remediation and development effort required measurable in a quantity of minutes to hours.
Remediation Suggestion	**This column provides a brief general or technical description of the suggested remediation path. This may include links to bug fixes or patch information. Other references or brief descriptions of typical remediation approaches.**

5. Project Management Approach

AT&T Cybersecurity Consulting understands the importance of project management in an engagement. The following details AT&T Cybersecurity Consulting's approach to project management. The same approach is used for each engagement, although certain tasks and documents may not be applicable or needed depending on the timeline, size and delivery of the project. The Project Lead or Project Manager from the AT&T Cybersecurity Consulting team, which may also be one of the consultants delivering work, will work closely with the DoIT team and/or project manager.

AT&T project management professionals use the globally recognized Project Management Institute's (PMI®) ANSI-approved and ISO 9001-approved standards and processes. The following paragraphs provide an overview of the AT&T project management methodology. It discusses our ability to deliver high quality, large-scale projects. The five high-level PMI® processes are:

- **Initiating**—recognizing that a project or phase should begin and committing to do so.
- **Planning**—devising and maintaining a workable scheme to accomplish the business need that the project was undertaken to address.
- **Executing**—coordinating people and other resources to carry out the plan.
- **Controlling**—ensuring that project objectives are met by monitoring and measuring progress and taking corrective action when necessary.
- **Closing**—formalizing acceptance of the project or phase and bringing it to an orderly end.

By using these very controlled processes and procedures, AT&T has been very successful in delivering projects on schedule and within budget. This clear process preserves budget and ensures that all time spent on the project by DoIT personnel is effectively used. Once AT&T becomes engaged, a comprehensive project plan based on PMI methodology will be used to manage and guide the project. The project plan will be tailored to the needs of the project and may include some of the following:

- **Vision Statement**—The vision is business-based and is focused upon the project objective: conduct network security vulnerability assessment and thereby strengthening the security posture of DoIT.
- **Project Charter**—The Project Charter is the starting point for the project as it provides initial high-level information about the project, assigns responsibilities,

and confirms the overall intent of the project. The program manager is responsible for making sure that the project charter exists and is complete.

- **Scope**—The scope statement provides a documented basis for making future project decisions and for confirming or developing common understanding of project scope among the stakeholders. The scope section is what outlines the project. This is what the project team will be expected to deliver to DoIT.
- **Work Breakdown Structure (WBS)**—Utilizing the completed scope statement, the project team develops the WBS. "A work breakdown structure is a deliverable-oriented grouping of project elements that organizes and defines the total scope of the project: work not in the WBS is outside the scope of the project. As with the scope statement, the WBS is often used to develop or confirm a common understanding of project scope" – (PMI ®). The entire project team, including those DoIT personnel working with the AT&T team, will be involved in the development of the WBS to make sure that all elements of scope are represented. The output of the WBS development exercise will be a significant level of detail about what work is to be done and will also create the WBS diagram.
- **Work Packages**—"The work package is the lowest level of the WBS" – (PMI ®). Work packages will be developed that are 8 to 80 hours in length, produce a specific product, have a definite beginning and end, are easily measured, and have natural sub-divisions. There is one work package for each of the lowest level elements of the WBS. All planning and analysis of the project is done at the work package level. Planning components include schedule, cost, quality, resources, communications, and risk.
- **Responsibility Matrix**—A responsibility matrix is used to closely link roles and responsibilities to the project scope definition. ". a high-level responsibility matrix may define which group or unit is responsible for each element of the work breakdown structure while lower-level matrixes are used within the group to assign roles and responsibilities for specific activities to particular individuals" – (PMI ®).
- **Quality Checklists & Metrics**—The most important part of quality is preventing problems in the project before they happen. The standard AT&T methodology is for the project team to develop checklists and metrics during the planning process and then use them during the execution and control processes. This technique provides a significant reduction in the number of quality issues and greatly increases the probability of overall success on the project.
- **Risk Identification and Mitigation**—The identification, quantification, development of mitigation plans, and control of risks is an ongoing process

throughout any AT&T project. Our principal aim is to identify, quantify, and respond to risks before they occur. During the development of the work packages, the project team will start the focus on risk by including the risk elements in the work packages.

- **Project Schedule**—Once the project team has completed and approved the work packages, they begin to roll the results into the appropriate portions of the project plan. After identifying, sequencing, and assigning durations, the project team then develops the baseline schedule to execute and control the project.
- **Communication Plan**—AT&T has a specific methodology around managing the communications on a project:
  - Communication is one of the most crucial aspects of project success.
  - We collaborate with the client to create, implement, and manage a communications plan to:
    - Provide positive understanding of the project
    - Provide essential progress of the project to appropriate stakeholders
  - Communication is planned into the project, with specific goals, objectives, deliverables, roles and responsibilities, and schedules. A communications team, consisting of associates involved in the planning of the project as well as representatives from the DoIT team will be tasked with the responsibility to design a plan that includes:
    - Scope, schedule, cost status reports including project performance measurement (trend, variance, earned value)
    - Risks and risk management issues
  - Key upcoming tasks, issues, and deliverables
    - Escalations
    - Quality
- Change Control—If there is a specific change to project scope, this change will be documented and agreed upon by both DoIT and AT&T before action is taken.
- Deliverable Procedures and Acceptance—AT&T utilizes a standard process to deliver each component of a project to our client by exercising a “Close Out” procedure for that deliverable. These Close Out activities perform two important functions:
  - Make the transition to the next phase of a project
  - Establish formal closure of a particular phase of a project.

The formal acceptance of a project deliverable, the reconciling of project accounts and the closing out of change logs and issue logs – all of these things bring the phase to completion.

6. Appendix: References

AT&T Cybersecurity Consulting has conducted similar assessments for many organizations. As a trusted advisor and partner, and as a professional courtesy to our clients, it is AT&T Cybersecurity Consulting's strict policy to not divulge contact references of our customer lists. This policy helps to protect our clients by limiting the circulation and data handling of their highly sensitive information. We assure DoIT that if we establish a business partnership, you will receive this same degree of respect and protection as a valued partner. AT&T Cybersecurity Consulting will be happy to provide this information to DoIT based on explicit consent from our current customers after this initial RFI phase to furnish evidence of our successful commitment to customer satisfaction.

In addition, readily available third-party industry ratings attest to our status as a leading Managed Security Services Provider (MSSP). For example, in its Magic Quadrant for MSSPs, Gartner has consistently positioned AT&T as a leader.

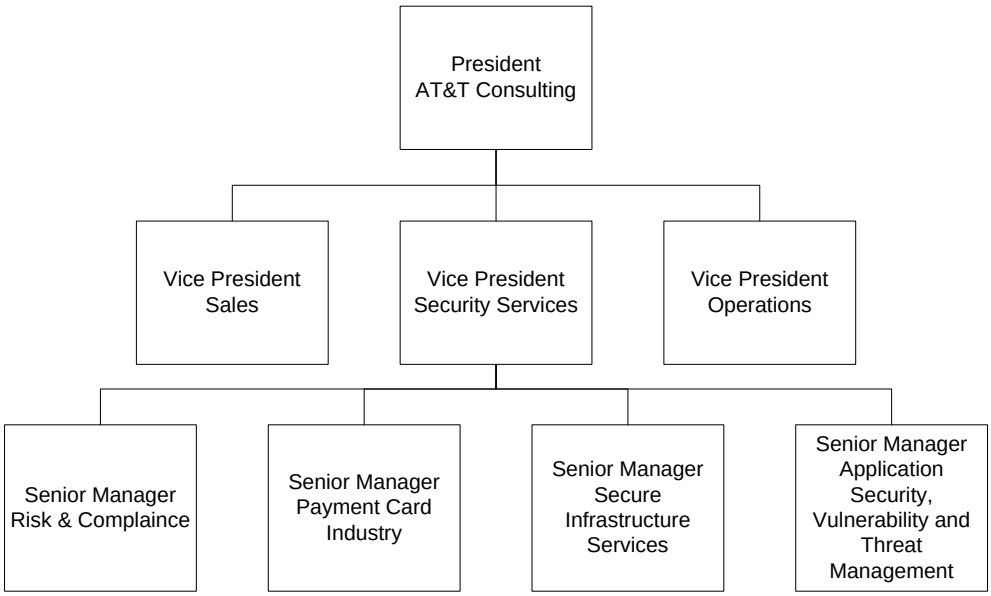
Among the aspects that differentiate AT&T from many MSSPs are

- An end-to-end approach–We provide security across the global enterprise.
- Layered, in-depth security strategy–We use our network's power to improve on traditional, premises-based security.
- Experience and expertise–Among our many projects, we've supported key U.S. Homeland Security initiatives. In 2007, the U.S. Department of the Treasury chose AT&T to build Treasury Network (TNet), its next-generation enterprise network.

So, we can demonstrate that we're a world-class managed security provider.

7. Appendix: Project Team Staffing and Sample Bios

AT&T has many individuals focused on security services; some of the larger teams include the Chief Security Office, Managed Security Services and the Security Services team within AT&T Cybersecurity Consulting. While all three groups work together, the AT&T Cybersecurity Consulting team would be delivering the assessment. The AT&T Cybersecurity Consulting organization organizational chart follows, along with a listing of many of the offerings for each practice line.



Upon award, AT&T Cybersecurity Consulting will work closely with DoIT to assign the best available resources for each aspect of the engagement. Because of the fluid nature of resource availability, it would be premature to assign specific resources at this time. Instead, we are providing representative bios of consultants who may be engaged with DoIT on this project.

Bio#1: JH, CISSP, CCSP, CCNA, MCSE

Background

JH is a security engineer with ten years of experience in designing and implementing technical solutions to support security initiatives for commercial and government organizations including the Department of Health, American Express, Bank of America, JPMorgan, Merrill Lynch, UBS, TWC, and Cablevision.

Over the years JH has delivered a variety of information security projects in network design, systems implementation, and software development. JH performed network and application penetration tests for major financial institutions and large telecommunication companies. She is currently engaged in cutting edge security research at a major national university.

JH possesses outstanding analytical abilities, excellent communication skills, and high work ethics.

Key Highlights & Skills

- Managed and delivered significant security projects
- Presented findings and recommendations to customers (reports and oral presentations)
- Analyzed software designs and implementations from a security perspective to uncover functional security flaws
- Conducted Payment Application Data Security Standard technical testing to assist software vendors in creating secure payment applications
- Performed external and internal penetration tests, network architecture and firewall assessments
- Designed and implemented network security management solutions and products
- Expertise knowledge of software reverse engineering
- Expertise knowledge of C/C++/C# and script-based programming languages
- Administered and maintained Windows and UNIX information technology systems

Certifications

- Certified Information System Security Professional (CISSP)
- Cisco Certified Security Professional (CCSP)
- Cisco Certified Network Administrator (CCNA)
- Microsoft Certified Systems Engineer (MCSE)

Education

- MS in Computer Science
- BS in Applied Mathematics

Bio# 2: DB, CISSP, CBCP

DB is a disciplined and motivated information security risk leader with deep operational knowledge and solid technical skills committed to the stewardship of systems and data and the growth of people and teams. She is a forward-thinking strategist with strengths in conceptualization and building consensus. Skilled at leading and understanding technical people and describing the results of these activities to business leaders in a context they can understand.

She provides security and risk consulting to clients in a broad spectrum of domains, including security assessments, risk management, compliance frameworks and strategic advisory services. She has led efforts to design and develop security programs for large corporations, developing cost-effective security program road maps that demonstrably improve the organization's maturity. She focuses primarily on financial organizations.

She helps organizations improve their resilience and compliance initiatives by managing, assessing and controlling risk enhancing the reliability of people, systems and processes. She protects the security of client financial assets and availability of operations by helping clients identify and manage risk and prepare for continued service in the face of disruptions. She ensures region specific regulatory compliance for information security and data privacy by driving compliance through corporate policies, standards and design criteria. DB has 20 years of experience in a wide array of information systems and information security disciplines.

<u>Key Highlights & Skills</u>

- Cybersecurity governance
- Cyber incident response, CSIRT and cyber exercise program development
- Business continuity planning, disaster recovery testing and business impact analysis (BIA)
- Security risk assessments: NIST CSF, SP800-30, 37, 53 rev4; ISO/IEC 27005:2011, 31010:2009, 27001 & 27002:2013; COBIT 5, OCTAVE Allegro, CIS CSC, FFIEC
- Implementing NIST Cybersecurity Framework with COBIT 5
- Qualitative & quantitative risk analysis
- Monte Carlo risk modeling
- Security & technology infrastructure documentation (Visio and other)
- Corporate policies, standards and design criteria
- Software security analysis reporting

- Threat modeling, data flow diagram (DFD), STRIDE threat ranking

Certifications and Training

- Certified Information Systems Security Professional (CISSP), ISC2
- Certified Business Continuity Professional (CBCP), DRII
- IT Security & Compliance (GDPR, Privacy Shield, Cloud Security)
- Network Security Tools (nMap, WireShark, NetworkMiner, MD5sum)

Education

- Master of Science, Information Security Leadership, Brandeis University

8. Appendix: Company Overview

AT&T includes more than 500 subsidiaries. You can find a list of our principal subsidiaries in our publicly filed 10K Report. The list includes the subsidiaries' legal names, states of incorporation/formation, and the names under which they do business (their DBAs). You can view the list at this website:

https://otp.tools.investis.com/clients/us/atnt/SEC/sec-show.aspx?FilingId=12564537&Cik=0000732717&Type=PDF&hasPdf=1

AT&T Corp., an AT&T Company, is the respondent for this proposal. The AT&T Corp. date of incorporation was March 3, 1885.

Company Overview

In the U.S. and Mexico, AT&T serves more than 156.6 million wireless subscribers, and is a premier provider of broadband, long distance, and local voice services. We also offer our communication services in almost every other country and territory in the world. Our services enable calls from more than 225 countries as well as wireless data roaming—for laptops, hand-held devices, and other data services—in more than 200 countries.

As a worldwide provider of IP-based services, we offer an extensive portfolio of Virtual Private Network (VPN) and Voice over IP (VoIP) services, which we back with security and support capabilities. We deliver these services to you via one of the world's most advanced backbone networks. Our wholly owned backbone network, which we operate from 36 Internet data centers (IDCs) on four continents, uses Multiprotocol Label Switching (MPLS) technology to integrate multiple network services.

The network provides MPLS-based services in nearly 200 countries and includes more than

- 3,800 nodes
- 1,142,562 fiber route miles

We also operate a wireless network that includes

- Coverage of more than 99% of the U.S. population, including the top 100 U.S. markets.
- Superior speeds for data and video services, as well as operating efficiencies using the same spectrum and infrastructure for voice and data on an IP-based platform.

- Digital transmission technologies known as GSM, General Packet Radio Services and Enhanced Data Rates for GSM Evolution for data communications.
- The nation's fastest mobile broadband network. 4G speeds are available with our Universal Mobile Telecommunications System/High Speed Downlink Packet Access (UMTS/HSDPA) broadband and HSPA+ network technology, combined with our upgraded backhaul.
- AT&T 4G LTE coverage to more than 400 million people in North America
- Ongoing deployment of HD voice on VoLTE (Voice over Long-Term Evolution) on a market-by-market basis

In addition to retail communication services, AT&T is a global leader in wholesale communication services. Our wholesale organization serves carriers, wireless service providers, systems integrators, cable providers, Internet service providers (ISPs), and content providers that need global, regional, and local end-to-end solutions.

A key to our success in providing and integrating services is AT&T Labs, our research and development group. AT&T Labs has won eight Nobel Prizes and has more than 12,500 patents. Our researchers and engineers developed some of the world's major technological inventions, including the transistor, solar cell, cell phone, and communications satellite. In addition, AT&T Labs led in developing DSL and other broadband Internet transport and delivery systems as well as wireless data networks.

You can find additional corporate information at the following link http://www.att.com/gen/investor-relations?pid=5711.

When you choose AT&T as your provider, you get innovative products and high-quality service.

Corporate History

In 1876, Alexander Graham Bell invented the telephone. That was the foundation of the company that would become AT&T – a brand that is synonymous with the best, most reliable telephone service in the world.

In 1984, through an agreement between the former AT&T and the U.S. Department of Justice, AT&T agreed to divest itself of its local telephone operations but retain its long distance, R&D, and manufacturing arms. From this arrangement, SBC Communications Inc. (formerly known as Southwestern Bell Corp.) was born.

Twelve years later, the Telecommunications Act of 1996 triggered dramatic changes in the competitive landscape. SBC Communications Inc. established itself as a global

communications provider by acquiring Pacific Telesis Group (1997), Southern New England Telecommunications (1998) and Ameritech Corp. (1999). In 2005, SBC Communications Inc. acquired AT&T Corp., creating the new AT&T.

With the merger of AT&T and BellSouth in 2006, and the consolidated ownership of Cingular Wireless and YELLOWPAGES.COM, AT&T is positioned to lead our industry in one of its most significant transformations since the invention of the telephone nearly 130 years ago.

Differentiators

Several factors differentiate AT&T from its competitors.

AT&T

- Is the world's largest communications company.
- Carries more than 197 petabytes of data traffic over its backbone network on an average business day.
- Has the best global coverage of any U.S. wireless provider with calling and texting available in over 225 countries and territories and discounted data coverage in over 200 countries and territories, including LTE speeds in over 100 countries and territories.
- Is a leading provider of wireless services in the U.S., with 141.6 million subscribers as of 4Q 2017.
- Has an IP broadband network covering more than 60 million customer locations.
- Owns and operates more than 48,000 hot spots in the U.S. and provides access to more than 1.2 million global hot spots.
- Is the world's largest TV provider and video distribution leader across TV, mobile, and broadband services.
- Wholesale delivers a full suite of industry-leading, white-labeled domestic and global network services, devices and applications to carriers, cable operators, content providers, wireless providers and ISPs.
- Owns an overall wireless voice and data network covering more than 99% of all Americans.

When you choose AT&T, you get a provider with a proven record of quality, service, and innovation.

Strategic Goals

AT&T's strategic goals focus on becoming the premier integrated communications company in the world by designing and deploying world-class wireless, fiber, and Internet Protocol (IP) networks to serve its customers.

To achieve those goals, we're committed to steady and consistent investment in the following initiatives:

- **Deliver an effortless customer experience**–When we design products, processes, or a user experience, we strive to build "effortless" into every touch point. To make "effortless" a competitive advantage requires continuous investment and improvement, to which we've allocated significant capital.
- **Lead in connectivity and integrated solutions**–Premier network assets are the foundation for delivering the integrated mobile, video, and data solutions you want. Our goal is to deliver seamless connectivity to every device and sensor in your offices, cars, and homes and make sure it's fast, highly secure, and reliable.
- **Produce and assemble world-class entertainment**–We're focusing on delivering that entertainment wherever, whenever, and however you want it. Via DIRECTV and other means, we can build truly differentiated entertainment services whether it's traditional TV, mobile, or over-the-top.
- **Serve our customers globally**–We continue to invest in integrated solutions that connect people and businesses around the world. To that end, we're transforming our network from hardware- to software-centric. This software-defined network makes it easier for us to offer our products globally and lead the industry in serving multinational businesses.
- **Operate with an industry**-leading cost structure–Our software-centric network transformation will enable us to deliver the most network traffic at the lowest marginal cost in the industry. In addition, we're streamlining operations, simplifying offers, getting the best prices from our supply chain, automating customer self-service, and making more interactions digital to reduce the time it takes to provide service.
- Equip our people for the future–We're using innovative training and building profiles of future job requirements to help our employees pivot their skills from hardware to software, from legacy wireline to mobile and entertainment, and from data recording to data science.

We strive to provide you with outstanding customer service and innovative technology.

About AT&T Cybersecurity Consulting

AT&T Cybersecurity Consulting offers a variety of infrastructure solutions that help our customers achieve competitive advantage. AT&T Cybersecurity Consulting has a heritage of delivering quality technology and business consulting to leading enterprises. Our life cycle services span strategic consulting and planning, through architecture & design, integration, and optimization. We deliver superior solutions by providing a broad base of services, a flexible, results-oriented engagement style, and the highest quality deliverables.

AT&T Cybersecurity Consulting services encompass the following six technology areas:

- **Convergence**—Provides forward thinking, robust and secure enterprise voice and data solutions. Our services help contain costs, enhance productivity, and provide investment protection for voice applications. Our offerings span the consulting life cycle and include planning services such as Telecom Strategy and IP Telephony Readiness, as well as Architecture, Integration, and Optimization of IPT and Contact Center solutions.
- **Advanced Infrastructure**—Provides clients with survivable, fault tolerant network infrastructure solutions that enable optimal, cost effective delivery of application services. Focus is in the areas of LAN/WAN, Wi-Fi and Mobility, Content Data Networking (IP Video), ATM/Frame, MPLS, QoS, and Optical internetworking.

- **Data Center**—Offers strategy, assessments, program planning and program management services in support of Data Center relocations and consolidations.
- **Security**—Our security services enable business enterprises to become more agile and competitive. We provide Trusted Advisory services, Secure Network Integration (FW/IDS/IPS), Compliance, Risk Assessments, Policy development, and traditional Vulnerability and Penetration testing.
- **Enterprise Operating Systems & Messaging**—Provides life cycle services for Enterprise Operating Systems and Messaging platforms, including Microsoft Technologies Consulting, IT Cost Cutting Initiatives focused on Server and Storage Consolidation, Server Virtualization, Identity and Access Management, Network Services, Messaging Design, and High Availability.
- **Network & Systems Operations Management**—Solutions addressing the technology, process (FCAPS and ITIL frameworks), and staffing dimensions of enterprise management across all infrastructure areas. Life cycle services include Strategy & Roadmap through software integration and operations optimization, and build-vs-buy analysis.

Differentiators

AT&T Cybersecurity Consulting provides these important and unique capabilities to our customers:

- **Experience**—Our consultants are experienced in deploying large and complex infrastructure solutions, and successfully integrating them into the existing environment. Our extensive background enables us to provide strategic guidance based on years of diverse project experiences.
- **Trusted Advisor**—AT&T Cybersecurity Consulting works as a part of our customer teams and as an advocate for their business interests. Our experience and certifications across leading solutions helps ensure successful multi-vendor integration. We offer independent validation, and optimization to realize cost savings.
- **Thought Leadership**—AT&T Cybersecurity Consulting has published over nine books on technologies including IP Telephony, IPv6, Security, and Virtualization. Our consultants are frequent speakers at industry recognized events and are recognized as Subject Matter Experts in their respective fields.
- **Structured Methodology**—Our proven, proprietary methodology helps ensure on-time and on-budget performance. We regularly optimize our own service specific methodologies with new intellectual capital, and delivery tools and templates which will provide additional customer value.

- **Holistic Approach**—In addition to technology considerations, we balance the people and process components as well. Our engagement approach factors in cross-disciplinary considerations, such as how to effectively secure and manage the client's infrastructure.

New Hampshire Public Television

Host: Richard Ager

Segment Aired: December 17, 2009

NHPTV Summary: Voting security became an issue in the 2000 election. We speak with Secretary Bill Gardner along with other guests to discuss the integrity and security of New Hampshire's voters.

Richard Ager: “This week, the Electronic Ballot Counting Device Advisory Committee issued its report.”

Quote from Harri Hursti in the New Hampshire Governor’s Council Chambers, in a meeting to present the results of the Electronic Ballot Counting Device Advisory Committee, filmed by New Hampshire Public Television:

“When I was inside the U.S., I would make a comment about the amount of checks and balances and the willingness to bring scrutiny over your own results. New Hampshire is doing more recounts than, I think… there is no one else doing as much recounts as New Hampshire.”

NHPTV Segment can be viewed at: https://video.nhptv.org/video/nh-outlook-voting-machines/

Dear Elections Assistance Commissioners and all interested parties:

We write this letter of concern and solution proposal after speaking with many members of the federal, state, and county governments. Thanks to EAC Director Hancock for encouraging this letter.

It is our assumed duty to again reach out in hope of providing information regarding election system security and best practice. The undersigned is a collective of concerned citizens and technologists focused on protecting our United States election systems from manipulation. Our represented group partially consists of technologists, solution providers and activists.

It is our understanding and conclusion that, as of this date, there has been little progress toward properly securing the election systems for the United States. This is the cause of our grave concern. It is our further conclusion and concern that although properly defensible election system technology is available for deployment, that technology is being deterred and delayed by corporations attempting to protect market share and shareholder interest to the detriment of the national security.

1. BACKGROUND

For context, in 2004 Open Voting Consortium demonstrated an open source election system: https://www.nytimes.com/2004/04/01/business/technology-briefing-software-voting-software-to-be-demonstrated.html

In 2005, the Government Accountability Office directed the technology transfer aspect of a National Science Foundation multi–million dollar grant (grantee ACCURATE) to include the open source pioneering work of Open Voting Consortium. This directive was ignored by the ACCURATE group and that grant money yielded no specific public benefit. Other disturbing activity has been noted attached to the ACCURATE absorption of the grant.

In 2006, Dr. Rebecca Mercuri filed documentation of inappropriate action by the ACCURATE working group with the NSF's Inspector General :

http://www.notablesoftware.com/ACCURATE/ACCURATE.html

This initial diversion away from open source voting systems caused substantial delay and altered the United States government's path toward proper election system security. To this day, the same controlling group from ACCURATE (i.e., David Dill -VERIFIED VOTING) has tendered opinion at the highest levels of government. Currently the affiliate network under VERIFIED VOTING (Center for American Progress , League of Women Voters, Lawyers Committee for Civil Rights, etc.) is properly touting audits and paper ballots, but improperly continuing to omit the necessary component of open source technology. This is hereby noted and the opinion assumed affected by corporate interests:

https://www.nytimes.com/2017/08/03/opinion/open-source-software-hacker-voting.html

http://www.sfexaminer.com/securing-u-s-election-systems-paper-ballot-isnt-enough/

Conversely, there has been election system security progress in the State of New Hampshire with Dr. Juan Gilbert's open source, paper ballot Prime lll system. The State of Ohio recently certified open source software for absentees and San Francisco County has allocated 1.7 million dollars toward the initial build-out of an open source election system project:

http://news.ufl.edu/articles/2016/05/how-universal-design-can-help-every-voter-cast-a-ballot.php

https://www.theregister.co.uk/2016/02/10/san_francisco_to_open_source_voting_systems/

2. INTERFERENCE WITH U.S. ELECTIONS

It is now generally acknowledged that the proprietary election systems sold by vendors to the United States via Help America Act funds are deficient and cannot be cured by the mere addition of a paper ballot or an after the fact audit. Though ballots and audits are ostensibly in the positive column, the position of experts is that the software cannot remain private and secret as "security by obscurity " is now recognized as a failed concept. The scientific position for open source software voting system security is further bolstered by the conclusions of NASA and the DOD. Experts omitting this piece of the security conversation must be questioned regarding source of motivation. Also, technologists devising new licenses under the banner of open source are likewise properly scrutinized for motivation. Los Angeles County has recently announced an "open source" system but has not revealed the software. See the Los Angeles County "open source voting" project:

https://statescoop.com/los-angeles-countys-new-open-source-vote-tallying-system-isnt-open-source-just-yet

It is fair to state some of the same experts omitting open source solutions to the election system crisis in advocacy work are also pushing for the purchase of yet another round of proprietary voting systems. This is an untenable position in the wake of the intelligence community findings of easily conducted interference with the proprietary systems.

3. OUTREACH TO GOVERNMENT FROM THE PRIVATE "DO-GOODER" SECTOR

The National Association of Voting Officials was formed as California Association of Voting Officials with a mission toward education and availability toward a public–private open source voting software quality assurance program. CAVO / NAVO and its preceding OVC has reached out to veritably ALL politicians and good government groups in the election security space for the purpose of heightening awareness and moving toward the deployment of solution voting systems. The response has been less than stellar as the time frame windows now close on our ability to secure the U.S. voting systems by 2020. Political will ebbs and flows as Microsoft and those government advocacy groups who "bob in their wake" continue to cause delay via fear, uncertainty and doubt tactics.

4. VENDORS SEEKING TO LOCK IN PRIVATIZATION OF ELECTIONS CONTINUE TOWARD FAILED SECURITY

https://motherboard.vice.com/en_us/article/mb4ezy/top-voting-machine-vendor-admits-it-installed-remote-access-software-on-systems-sold-to-states?utm_campaign=sharebutton

https://www.yahoo.com/news/former-trump-official-no-one-minding-store-white-house-cyberthreats-090017630.html

5. LOS ANGELES COUNTY

As the U. S. largest jurisdiction, many have awaited the unveiling of the new Los Angeles voting system. Though the design is less than optimal as it is based in proprietary hardware (with reference appropriate to the sole source contracts inherent), the promised software is open source. Unfortunately, as of the date of this letter, Los Angeles County has not evidenced their claims that the voting system will actually be open source as defined by Open Source Initiative and other recognized authorities. The EAC should also make public statement that the definition of open source is in keeping with the OSI definition: https://opensource.org/osd-annotated

More specifically, the following language in a proposed California ballot measure for 2020 (Election Transparency and Security Act of 2020) includes the meaning of open source voting. Please see clauses Ch.5, Article 1, 19401 of the measure:

(c) "Open source software" means software actually distributed to the public under software licenses that provide that every licensee is free to make copies of the software or derivative works thereof, to distribute them without payment of royalties or other consideration, and to access and use the complete source code of the software.

(d) "Open source voting system" means a voting system that uses open source software for all voting-specific components.

6. CONCLUSIONS AND SOLUTIONS

Based on the above statements the undersigned are agreed that the security interests of the United States of America are best served by the immediate creation, certification and deployment of General Public License open source election systems to replace proprietary voting systems. These open source voting systems should be deployed (with paper ballots and robust audits) as soon as possible. The Elections Assistance Commission should waive (as a national emergency) any and all fees for such systems to apply for and complete immediate certification.

Also, The EAC, NIST, DNI, DHS, and all other relevant bodies should convene in an emergency setting to devise best methods of creating public-private partnerships for the said purpose of the aforementioned open source voting system deployment. The EAC should also, as stated in section 5 herein, make public statement that the definition of open source is in keeping with the OSI definition.

Respectfully submitted,

Brent Turner
Secretary
California Association of Voting Officials

Daniel J Cloutier

From: Anthony Stevens
Sent: Monday, September 10, 2018 9:15 AM
To: Daniel J Cloutier; tomandnanmanning@comcast.net; Colleen McCormack
Subject: FW: Moratorium on voting system purchases / leases- EAC letter
Attachments: EAC letter.pdf

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Karen Ladd
Sent: Monday, September 10, 2018 8:26 AM
To: Anthony Stevens
Subject: FW: Moratorium on voting system purchases / leases- EAC letter

From: Brent Turner [mailto:turnerbrentm@gmail.com]
Sent: Friday, September 07, 2018 2:14 PM
To: elections.sos@state.or.us; jim.bennett@sos.alabama.gov; Mead Treadwell; administrator@asg-gov.net; AZSecState; info@sos.arkansas.gov; secretary@sos.state.co.us; denise.merrill@ct.gov; Kathy Bradford; secretary@dc.gov; dossecretaryofstate@dos.myflorida.com; sos@sos.ga.us; service@guam.gov; ltgov@hawaii.gov; secstate@sos.idaho.gov; jessewhite@ilsos.net; sos@sos.in.gov; SOS Email Account; sos@sos.ks.gov; sos.secretary@ky.gov; admin@sos.la.gov; Office, SOS; mdsos@sos.state.md.us; cis@sec.state.ma.us; secretary@michigan.gov; secretary.state@state.mn.us; delbert.hosemann@sos.ms.gov; info@sos.mo.gov; sos@mt.gov; sos.info@nebraska.gov; sosmail@sos.nv.gov; Karen Ladd; lt.governor@gov.state.nj.us; diannaj.duran@state.nm.us; info@dos.ny.gov; emarshal@sosnc.com; sos@nd.gov; jhusted@ohiosecretaryofstate.gov; webmaster@sos.ok.gov; oregon.sos@sos.or.us; ST-PRESS@pa.gov; armollis@sos.ri.gov; Renee Daggerhart; sdsos@state.sd.us; Tre Hargett; secretary@sos.state.tx.us; spencercox@utah.gov; jim.condos@sec.state.vt.us; sonia.boyce@lgo-vi.gov; socmail@governor.virginia.gov; kim.wyman@sos.wa.gov; wvsos@wvsos.com; doug.lafollette@sos.state.wi.us; secofstate@wyo.gov
Subject: Moratorium on voting system purchases / leases- EAC letter

Dear U.S. Election Officials :

As you know, for many years, we have been providing information to the U.S. jurisdictions and counties regarding best methods to defend against voting system interference.

Unfortunately it has taken a national security crisis to garner attention to open source election systems and solutions. These publicly owned systems are half the cost and twice the security of the current vendor sold " proprietary " models. A proper system is now deployed in New Hampshire and slated for build out in San Francisco. We now call for a moratorium on purchases or leases of the current vendor models based on obvious recent events as well as previous government study.

https://www.nytimes.com/2017/08/03/opinion/open-source-software-hacker-voting.html

For smaller counties the open source funding will be crucial, but we still need political will and education. Counties should reach out to San Francisco County or NAVO for more information. NAVO encourages pooling of resources.

There are better publicly owned systems on the horizon. Please reject all pressures to purchase / lease the current batch of security deficient / over-priced systems

Best regards,

Brent Turner

www.navo-us.org

650-726-1133

General article regarding hacks https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections

Daniel J Cloutier

From: Orville Fitch
Sent: Saturday, June 15, 2019 5:32 PM
To: David Scanlan; Anthony Stevens; Daniel J Cloutier; Colleen McCormack
Subject: Interesting Politico Story on EAC

HTTPS://WWW.POLITICO.COM/STORY/2019/06/15/FEDERAL-ELECTION-BRIAN-NEWBY-2020-1365841?FBCLID=IWAR33ODP_FMOXWH2DOFSQN1K0BHXQCERVHMTYTYO5IEUEUIIJXNHD1FRKNSA

Federal election official accused of undermining his own agency - POLITICO

www.politico.com

Troubles at the Election Assistance Commission could undermine the effort to safeguard the 2020 presidential contest from foreign meddling.

CYBERSECURITY

Federal election official accused of undermining his own agency

Troubles at the Election Assistance Commission could undermine the effort to safeguard the 2020 presidential contest from foreign meddling.

By ERIC GELLER

06/15/2019 06:36 AM EDT

A tiny federal agency that plays a crucial role in assisting the nation's local election supervisors is gripped by a leadership crisis that has sparked concerns that it is unprepared to play its role in protecting the 2020 presidential race from foreign interference.

Brian Newby, the executive director of the Election Assistance Commission, has blocked important work on election security, micromanaged employees' interactions with partners outside the agency and routinely ignored staff questions, according to former election officials, former federal employees and others who regularly work with the agency.

In doing so, Newby has not only frustrated his own employees and helped create a staff exodus — nine EAC office directors have left since Newby arrived — but also angered cybersecurity experts, election integrityactivists and state and local officials. His reputation in the elections community conjures up "the eye-roll emoji," said one former election official. "Everybody kind of puts up with him."

POLITICO's seven sources — all of whom requested anonymity to speak candidly — described Newby, a Republican, as too beholden to the EAC's GOP chairwoman, Christy McCormick, who masterminded his appointment and later spent years denying the reality of Russian interference in the 2016 election. They also said that Newby alienated his agency almost immediately by wading into the issue of a citizenship requirement for voter eligibility — and that he has failed to regain their trust ever since.

Sen. Ron Wyden (D-Ore.), one of the lawmakers most focused on election security, told POLITICO that “if these allegations are true, Brian Newby should immediately resign.”

Brian Newby, executive director of the Election Assistance Commission, disputed reporting on his alleged blocking the agency from doing its work. | Yorktel/U.S. Elections Assistance Commission via AP

“Our elections are too important for the Election Assistance Commission to be led by someone under the cloud of scandal and rampant mismanagement,” he said in a statement, referring in part to criticism over Newby’s tenure as election commissioner in Johnson County, Kan.

Newby disputed the complaints in an interview, defending his actions and saying the agency under his leadership had come a long way from its backwater status. McCormick has regularly praised Newby, including defending him from lawmakers’ criticism.

The troubles comes at a time of turmoil for other federal agencies responsible for defending critical U.S. computer networks from foreign hackers. The White House’s Office of the Federal Chief Information Officer is planning a reorganization this summer after POLITICO reported on complaints of infighting, high turnover and cratering morale. The Department of Homeland Security, which works with state election offices to secure their networks, has no permanent leader after former chief Kirstjen Nielsen resigned in April.

Newby’s work as the EAC’s top administrator has come under increasingly intense scrutiny from lawmakers as the end of his four-year term approaches in November. Lawmakers are considering whether to boost the agency’s budget in response to mounting election security threats, but sources said that more money and staff won’t matter as long as Newby remains in place.

House Administration Chairwoman Zoe Lofgren (D-Calif.), whose committee oversees

the commission, agreed with Wyden that it was time for "new leadership" at the agency.

"The EAC has tremendous potential to be a credible resource that election officials can trust in times of need," Lofgren said in a statement. "However, gross mismanagement from executive leadership cannot be allowed to derail the important mission of this agency."

Roadblocks and radio silence

When Congress created the EAC after the 2000 presidential election's hanging-chads debacle, lawmakers gave it a simple mission: Serve as a clearinghouse for best practices about election administration and prepare the Voluntary Voting System Guidelines, which many states have chosen to adopt as regulations.

The EAC's four commissioners are the agency's political leaders, making policy decisions like approving major voting-system guidance. The executive director is a career employee who supervises the staff and presents their work to the commissioners.

Russia's 2016 interference dramatically raised the profile of the agency and its work, forcing it to make election security a priority and spurring calls to boost its budget and staff.

But at a time when the EAC should be leaning into its election security mission, Newby has repeatedly blocked action, two critics of his work told POLITICO.

They said Newby has occasionally told staff not to work on cybersecurity best-practices

documents for state and local election officials — crucial guidance that many officials rely on as they run their elections. “The executive director was not supportive of them and put [up] roadblocks,” one former federal employee said.

“It was constant frustration,” said a second former government employee familiar with the tensions.

Newby has also prevented staff from participating in election security events, like conferences, panels and training sessions. The second former employee described hearing from EAC staffers who said, “We’d like to do this with a conference, but Brian says no.”

In addition, he often provides “zero response to direct questions,” said the first former employee. Sometimes, they said, EAC staffers will proceed with the work anyway, leading to “direct reprimands” from Newby. Employees fear that if they do certain work, “they’re going to get in trouble,” said the former employee.

During an interview in his office at the commission’s headquarters in Silver Spring, Md., Newby repeatedly disputed and questioned POLITICO’s reporting about the concerns.

He said he couldn’t respond to the claim about him blocking work on best-practice documents “without knowing what those documents are.”

He said he wasn't "aware" of having stopped work on any initiatives.

Regarding his efforts to keep staff from participating in conferences and events, he said, "I don't know what that's referring to," though he pointed out that he may have made some travel decisions because of budgetary constraints.

McCormick defended Newby during a May 21 hearing of the House Administration Committee. "I think that Mr. Newby is doing a fine job," she said. "It's unfortunate that there are some people who are attacking him." Asked about internal dissatisfaction, she said "unhappy" employees "have left the agency."

Wyden told POLITICO that McCormick "needs to end her unconditional support for this scandal-plagued official."

Senate Rules Chairman Roy Blunt (R-Mo.), whose panel oversees the EAC, said in a statement that the agency "has a responsibility to ensure that the employees that it appoints are doing their jobs."

Despite the issue's importance, Newby has never made a priority of election security, four people knowledgeable about his work told POLITICO.

One voting security researcher described briefing Newby on an issue and hearing Newby promise to tell the commissioners about it. Two months later, the researcher talked to the commissioners and discovered that Newby never briefed them.

“I have stopped using him as an information conduit to the agency as a consequence,” the researcher said.

Newby also doesn’t fully understand election security or why it’s important, said two former election officials.

The voting security researcher recalled talking to Newby about a plan by Microsoft to develop secure electronic voting technology. “He was gobsmacked and kind of suspicious — like, ‘Why would a large corporation care about stable democracies?’”

‘Fifth commissioner’

Seeking to control the agency’s every action, Newby has micromanaged staff interactions with people and agencies outside the EAC, two of the people said. He repeatedly describes himself as “the face to other agencies,” said a former government employee, and tells staff that “nobody should be talking to outside entities without his awareness and/or his approval.”

Newby doesn’t trust his employees “to have meaningful conversations that don’t include him,” said a former election official.

Newby told POLITICO that he wants and deserves to be “aware of what’s going on in the agency,” especially when it comes to relationships with external partners like other agencies. In some cases, he said, staff might not be aware that an issue relates to “a high-level discussion” that commissioners have asked about; in those cases, it would be his role to monitor that work for the commissioners.

“Of course I’d want to have some insight into what’s going on,” he said. “I think that’s only reasonable.”

Asked about further complaints that he has ignored employees’ questions, Newby said, “I’m sure there’s times that I haven’t responded to somebody who’s asked for some guidance, just because we’re busy.”

2020 ELECTIONS

DNC, NBC announce first debate lineups

By ZACH MONTELLARO and CHRISTOPHER CADELAGO

His critics say Newby has also failed to effectively mediate between EAC commissioners and staff, one of the executive director’s main jobs. Instead, said the election integrity expert and a former election official, Newby is trying to be a “fifth commissioner.”

“He’s a bit too deferential [and] doesn’t push back,” said the expert.

As a result, this person said, employees don’t feel appropriately insulated from the EAC’s political decision-makers.

Asked about the “fifth commissioner” idea, Newby said he would “have to know more about who said that” in order to answer.

Staff departures

The steady staff exodus received heightened attention with the departure in May of Ryan Macias, the acting director of testing and certification. Macias had replaced Brian Hancock, who had been testing director since

the EAC launched in 2003 but had left in March.

Newby's behavior played a big role in Macias' exit, three people told POLITICO.

Macias and Hancock's departures "knocked the wind out of the technical sails of the EAC," said the voting security researcher.

The responsibilities of the nine office directors who left cover almost every part of the agency, from research and testing to policy and human resources. A former government employee said Newby "was a major factor in the majority of the people that have left … since he got there."

Newby said that he couldn't "speak to why people have left" but that he hadn't "heard someone say they left out of frustration [with] me."

Employee survey data underscores the frustrations. Between 2016 — Newby's first full year as executive director — and 2017, the percentage of employees who expressed satisfaction with senior leaders' "policies and practices" dropped 23 points.

Asked about the data, Newby said it also applied to the commissioners and pointed to the unpopular departure of former commissioner Matt Masterson, saying it "happened right around the time of that survey." But Masterson left in March 2018, long after the survey was conducted.

The staff departures may continue. Several junior staffers on the research team "have been considering their next steps," said the election integrity expert.

The House aide bemoaned the exodus. “There are talented people … who want to do their job, who are dedicated public servants, and who are so deeply frustrated and put off by the executive director’s leadership style that they’re hemorrhaging talent.”

A rocky start

Newby was no one’s first choice to serve as executive director. But in 2015, as the EAC’s advisory boards considered a list of candidates, a split emerged between those who wanted someone with federal leadership experience and those who preferred someone with election administration expertise. Newby ended up as “a compromise candidate,” said one former election official.

McCormick badly wanted to hire Newby, but she needed the votes of the other two commissioners. So she floated a deal, three people knowledgeable about the matter said. To win over Thomas Hicks, she proposed that the EAC simultaneously hire Cliff Tatum, a Democrat whom Hicks liked, as the agency’s general counsel.

Hicks agreed, leaving Masterson with a choice: Accept the deal or leave the EAC without an executive director. Masterson went along with the deal. In November 2015, the EAC hired Newby and Tatum for four-year terms. Masterson did not respond to a request for comment.

The problems started almost immediately. In February 2016, Newby took the action for which he is best known: He approved requests

from Georgia, Alabama and his home state of Kansas to require residents filling out the federal voter registration form to prove they were citizens. Hicks blasted the move, saying it "contradict[ed] policy and precedent."

An appeals court later froze Newby's action, but the move forever poisoned his reputation among people dealing with the EAC, four sources said.

TECHNOLOGY

'Nightmarish': Lawmakers brace for swarm of 2020 deepfakes

By CRISTIANO LIMA

"That really just killed his credibility with a good number of election officials," said one former election official.

Many lawmakers and EAC staffers thought Newby "overly politicized his role," said the election integrity expert.

In the interview, Newby denied that his decision was about proof of citizenship, saying he was merely trying to "compare state instructions to federal instructions." He argued that the criticisms in POLITICO's story were "related to a political attack because of the proof-of-citizenship thought."

Newby doesn't regret his decision. "I made the correct decision, the only one I could do by law," he said.

Later in 2016, Newby's troubles deepened. The Associated Press reported that it had obtained documents that revealed that as Johnson County election commissioner, he had "berated employees," "deliberately bypassed supervision" and had an affair with a

subordinate that he used to cover up “lavish” taxpayer-funded trips and equipment purchases.

As the story emerged, said one former election official, “there were a lot of [people] on the [EAC advisory boards] that … wished they had known” about his scandals before he was hired.

‘Most people want to see him gone’

People who regularly deal with the EAC describe Newby as alternately infuriating or irrelevant.

One former election official recalled, “If we needed something, we’d either go to one of the commissioners or to whoever the relevant staffer was.”

Newby rarely attends events to represent the agency, the election integrity expert said, describing this as unusual for an executive director.

“If you asked most people, ‘Does Brian Newby provide value to you in your job?’” said one former election official, “you would probably get, ‘Who’s Brian Newby?’ or ‘No.’”

The House aide was more blunt: “His reputation is poor and most people want to see him gone.”

But getting rid of Newby won’t be easy, thanks to his close relationship with McCormick. In recent congressional testimony, she has advanced what two sources called a dubious theory: The EAC legally cannot begin searching

for a new executive director until the position becomes vacant in November.

2020 ELECTIONS

The winners — and losers — of the Democratic debate draw

By DAVID SIDERS and CHRISTOPHER CADELAGO

The EAC's founding statute, the Help America Vote Act, is not clear on this point. "I don't know what she's basing it on," said one former election official.

McCormick's decision to block a search process is a cynical ploy, according to the House aide. If the EAC doesn't have a list of candidates by the time Newby's term expires, the aide said, McCormick will pressure the other commissioners to reappoint Newby rather than leaving a vacancy three months before the first 2020 presidential primaries.

"She's creating a fake crisis in order to preserve him," the aide said.

But it is unclear whether Hicks would vote for Newby again after his proof-of-citizenship controversy. During the House hearing, Hicks described Newby's future as "something that the commission should look at."

Newby's top priority right now is keeping his job, said four of the people POLITICO spoke with for this story. "That's why … he's so deferential to the commissioners," said the election integrity expert. "He needs to keep them happy."

Newby acknowledged that he wanted to be reappointed. "I think I've done a really good job, and I think our staff has done a really good job," he said, adding that the EAC had

experienced “a pretty big turnaround” under his leadership. “So yeah, I’d like to continue the work.”

Missing momentum

As Newby and McCormick weigh the odds of his reappointment, EAC employees and outside groups are left wondering where this leaves the agency as its partners gear up for 2020. Multiple people said that between staff shortages, low morale and a lack of guidance from Newby, the EAC is ill-prepared to fully participate in this process alongside DHS and the FBI.

Newby “doesn’t have experience or energy to use the agency that he’s in charge of and the power that he has to improve what happened the last time,” said a former election official.

The irony, sources said, is that the EAC has never had a better opportunity to prove its worth. It survived years of Republican defunding threats and is close to finishing the landmark VVSG 2.0 update.

“This is really the moment that the EAC should be much more high-profile, and they’re missing the opportunity,” said an election integrity expert. “As we’re going into 2020, this is the time where they should be getting that attention, and there is no plan for that.”

NuHarbor Security
39 River Road, Suite 4
Essex Junction,, VT 05452 US
(800) 917-5719
finance@nuharborsecurity.com
www.nuharborsecurity.com

NuHarbor SECURITY

INVOICE

BILL TO

New Hampshire Sectretary of State
Attn: Paula Penney
State House, Room 204
107 Main Street
Concord, NH 03301-4989

INVOICE # NHSOS0718-03
DATE 07/24/2018
DUE DATE 08/23/2018
TERMS Net 30

PO
NHSOS-19-SW04

ITEM	DESCRIPTION	QUANTITY	RATE	AMOUNT
CS.EPPADV.SOLN.T3	EPP Advanced (Prevent + Insight + Discover) - Band 3	370	23.23	8,595.10
CS.OW.SVC.T3	Falcon Overwatch Service- Band 3	370	6.35	2,349.50
CS.PE.07	Falcon Platform - Standard Retention (7 Day)	370	6.72	2,486.40
CS.EPPCOMP.SOLN	EPP Complete	370	78.43	29,019.10
CS.DEVICE.SOLN	Falcon Device Control	370	2.12	784.40

REMIT CHECKS TO:
NuHarbor Security Inc.
39 River Road, Suite 4
Essex Junction, VT 05452

BALANCE DUE **$43,234.50**

CROWDSTRIKE

032-NES-3991216-

003691

NuHarbor Security
P.O. Box 51958
Boston, MA 02205 US
(800) 917-5719
finance@nuharborsecurity.com
www.nuharborsecurity.com

NuHarbor SECURITY

INVOICE

BILL TO

New Hampshire Sectretary of State
Attn: Paula Penney
State House, Room 204
107 Main Street
Concord, NH 03301-4989

INVOICE # NHSOS0718-01
DATE 07/09/2018
DUE DATE 08/08/2018
TERMS Net 30

AGREEMENT
NHSOS-IT-2018-002 PO

RESOURCE	ACTIVITY	DAYS	RATE	AMOUNT
PS-SPLD-NH	Splunk base configuration, data onboardinig, dash boarding and health check activities June 25 - 29, 2018 Dan Potter	5	1,800.00	9,000.00

REMIT CHECKS TO
NuHarbor Security Inc.
P.O. Box 51958
Boston, MA 02205

BALANCE DUE **$9,000.00**

Splunk
Corp Eligible
OK to Pay
8/9/2018

032-NES-3983558-

003692

NuHarbor Security
P.O. Box 51958
Boston, MA 02205 US
(800) 917-5719
finance@nuharborsecurity.com
www.nuharborsecurity.com

INVOICE

BILL TO

New Hampshire Sectretary of State
Attn: Paula Penney
State House, Room 204
107 Main Street
Concord, NH 03301-4989

INVOICE # NHSOS0718-02
DATE 07/10/2018
DUE DATE 08/09/2018
TERMS Net 30

VENDOR PO
NHSOS-18-SW60
OK

P.O. ~~NHSOS-19-SW04~~

DESCRIPTION	HOURS	RATE	AMOUNT
TAP URL Defense & AttDef, TAP Dashboard, Dynamic Reputation, Spam, Virus Protection, ZeroHour Anti-Virus, Email Firewall, Impostor email, greymail filtering, Smart Search - F-Secure - SaaS 1 to 250 12 Months Users 125 Proofpoint, Inc	1	19,687.50	19,687.50
Proofpoint Platform (MTA) with Email Protection and TAP Configuration (SaaS or On-Premise Appliance) 1 to 5000 Users 125 Proofpoint, Inc.	1	0.00	0.00
Platinum Level Support - SME - 12 Users 125 Proofpoint, Inc	1	0.00	0.00

REMIT CHECKS TO:
NuHarbor Security Inc.
P.O. Box 51958
Boston, MA 02205

BALANCE DUE **$19,687.50**

Proof Point
eMail
Arnold Sarkis

OK to Pay
Corp Eligible
Denise J. Hawkes
2/9/2018

032-NES-3983555-

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Friday, May 31, 2019 12:31 PM
To: Paula Penney
Subject: Election Related Cybersecurity Bills - Funding Sources

Paula,

Reading Anthony's email below, it looks like Bill has indicated that we will be paying cyber expenses related to HAVA out of Corp to make the required "match" … so that last Splunk P.O. I sent over today should be a Corp expense assigned as a "match".

Thanks,

Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>
Sent: Tuesday, May 21, 2019 5:10 PM
To: Nancy Swett <Nancy.Swett@SOS.NH.GOV>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: David Scanlan <David.Scanlan@SOS.NH.GOV>; Paula Penney <Paula.Penney@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: Election Related Cybersecurity Bills - Funding Sources

Nancy and Dan,

Please use this communication as your instructions to use Corporation Division information technology funds to pay election-related bills incurred in Federal Fiscal Year 2019 for cybersecurity services from Falcon/Crowdstrike, Proofpoint, Fireeye/Groupsense, and Splunk, as well as election-related bills for penetration testing and compromise assessment services, until the total amount of such payments reaches $155,113. When this threshold is attained, these expenditures will constitute the required state match for the 2018 Election Reform Program funds provided by Congress, and we should record these payments and enable federal reporting accordingly. After this threshold has been reached, please charge subsequent election-related cybersecurity bills to the Election Fund.

To the extent possible, please execute this before the 2019 State Fiscal Year-end, and advise me when the above threshold for the state match has been reached, with a status report on June 20, 2019 in any event. Thank you.

Anthony Stevens

Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Tuesday, May 21, 2019 5:10 PM
To: Nancy Swett; Daniel J Cloutier
Cc: David Scanlan; Paula Penney; Orville Fitch
Subject: Election Related Cybersecurity Bills - Funding Sources

Nancy and Dan,

Please use this communication as your instructions to use Corporation Division information technology funds to pay election-related bills incurred in Federal Fiscal Year 2019 for cybersecurity services from Falcon/Crowdstrike, Proofpoint, Fireeye/Groupsense, and Splunk, as well as election-related bills for penetration testing and compromise assessment services, until the total amount of such payments reaches $155,113. When this threshold is attained, these expenditures will constitute the required state match for the 2018 Election Reform Program funds provided by Congress, and we should record these payments and enable federal reporting accordingly. After this threshold has been reached, please charge subsequent election-related cybersecurity bills to the Election Fund.

To the extent possible, please execute this before the 2019 State Fiscal Year-end, and advise me when the above threshold for the state match has been reached, with a status report on June 20, 2019 in any event. Thank you.

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Monday, January 28, 2019 1:04 PM
To: Daniel J Cloutier
Subject: Election Security Improvements Back-up Needed

Dan,

As a first priority, I need supporting expense items for – Election Security Improvements - $97,066.11:

I would still like to see the back–up for all 3 of the 2018 totals shown below, with subtotals for personnel and non-personnel expenses:

Title I 2018	Voting Systems	SVRS	Admin Complaint	Prg Mgmt	Educ & Training	Polling Place	Election Tech	Security Improve	Total
2018	0.00	0.00	0.00	0.00	12,333.44	0.00	20,026.59	97,066.11	129,426.14
Match	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2019	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
To Date	0.00	0.00	0.00	0.00	12,333.44	0.00	20,026.59	97,066.11	129,426.14
Match	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
To Date	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2020	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
To Date	0.00	0.00	0.00	0.00	12,333.44	0.00	20,026.59	97,066.11	129,426.14
Match	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
To Date	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
2021	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
To Date	0.00	0.00	0.00	0.00	12,333.44	0.00	20,026.59	97,066.11	129,426.14
Match	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
To Date	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00

Cash Flow | Title I Cumm | Title I Hoz | Title I Vert | Title I Mth | Title I 2018 Cumm | Title I 2018 Mth | Title II Cumm | Title II Hoz | Title II Vert

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Monday, January 14, 2019 9:12 AM
To: Daniel J Cloutier; Nancy Swett
Subject: RE: Transfers - Falcon, Splunk, Proofpoint

Thanks, Dan.

Let's transfer Proofpoint and Falcon charges.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Daniel J Cloutier
Sent: Monday, January 14, 2019 8:42 AM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Subject: RE: Transfers - Falcon, Splunk, Proofpoint

Anthony,

I cannot support the movement of the NuHarbor Splunk Invoice for two primary reasons; the work was done 1) prior to the funds being received and 2) not directly in the interest of cybersecurity for the elections infrastructure. The other two invoices, CrowdStrike Falcon Complete and ProofPoint are more aligned with keeping our elections infrastructure secure.

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens
Sent: Friday, January 11, 2019 10:23 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Subject: Transfers - Falcon, Splunk, Proofpoint

Nancy and Dan,

Dave has told me he wants these cybersecurity expenses paid from the “Title I – New” account. Showing them as an FFY 2019 expense in “Title I - New” is the only way to do this that I know of.

They were all August, 2018 invoices that were approved in August, 2018, so this transfer can be accomplished within current SFY 2019.

Thanks.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Monday, January 14, 2019 8:42 AM
To: Anthony Stevens; Nancy Swett
Subject: RE: Transfers - Falcon, Splunk, Proofpoint

Anthony,

I cannot support the movement of the NuHarbor Splunk Invoice for two primary reasons; the work was done 1) prior to the funds being received and 2) not directly in the interest of cybersecurity for the elections infrastructure. The other two invoices, CrowdStrike Falcon Complete and ProofPoint are more aligned with keeping our elections infrastructure secure.

Thanks,

Dan
Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens
Sent: Friday, January 11, 2019 10:23 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Subject: Transfers - Falcon, Splunk, Proofpoint

Nancy and Dan,

Dave has told me he wants these cybersecurity expenses paid from the "Title I – New" account. Showing them as an FFY 2019 expense in "Title I - New" is the only way to do this that I know of.

They were all August, 2018 invoices that were approved in August, 2018, so this transfer can be accomplished within current SFY 2019.

Thanks.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way

Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Friday, January 11, 2019 12:12 PM
To: Daniel J Cloutier; Nancy Swett
Subject: FW: Transfers - Falcon, Splunk, Proofpoint
Attachments: NH Harbor Falcon.pdf; NH Harbor Splunk.pdf; NU Harbor Proofpoint.pdf

These would all be placed in J8 in "Title I – New" in FFY 2019, except that Dan still has to confirm the NU Harbor Splunk charge for applicability.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Anthony Stevens
Sent: Friday, January 11, 2019 10:23 AM
To: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>; Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Subject: Transfers - Falcon, Splunk, Proofpoint

Nancy and Dan,

Dave has told me he wants these cybersecurity expenses paid from the "Title I – New" account. Showing them as an FFY 2019 expense in "Title I - New" is the only way to do this that I know of.

They were all August, 2018 invoices that were approved in August, 2018, so this transfer can be accomplished within current SFY 2019.

Thanks.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Friday, January 11, 2019 10:23 AM
To: Daniel J Cloutier; Nancy Swett
Subject: Transfers - Falcon, Splunk, Proofpoint
Attachments: NH Harbor Falcon.pdf; NH Harbor Splunk.pdf; NU Harbor Proofpoint.pdf

Nancy and Dan,

Dave has told me he wants these cybersecurity expenses paid from the "Title I – New" account. Showing them as an FFY 2019 expense in "Title I - New" is the only way to do this that I know of.

They were all August, 2018 invoices that were approved in August, 2018, so this transfer can be accomplished within current SFY 2019.

Thanks.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Monday, December 17, 2018 11:12 AM
To: Anthony Stevens; Nancy Swett
Subject: RE: Correction - hava expenditures July through November

See below for a couple comments from me …

Thanks,
Dan

Daniel J Cloutier
Assistant Secretary of State
New Hampshire Department of State

Information Technology Office
NH State Archives - Room 209
9 Ratification Way, Concord, NH 03301
Phone: 603.271.0001 - Fax: 603.271.8242

From: Anthony Stevens
Sent: Monday, December 17, 2018 11:04 AM
To: Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Cc: Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Subject: Correction - hava expenditures July through November

Nancy,

Correction. As for the $67,681 payment to Software House International for Dark Web Monitoring, **we should allocate it to Dan's new category "J8" (Election Security Improvements) in the 2018 HAVA Funds.**

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Anthony Stevens
Sent: Friday, December 14, 2018 6:24 PM
To: Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Subject: FW: hava expenditures July through November

Nancy,

See below chart for changes I made today.

Changes today are in blue background. Changes yesterday are in yellow background. Both are valid for now.

I am not sure if the two file cabinets used for AVS storage and perhaps surplused (??) to White Farm on 8/14/2018 should appear as a charge of $80 to us. The file cabinets were not surplused to White Farm but purchased from White Farm to store the AVS tablets. The legal file cabinets are now the wall in the training room.

Also, I am not sure I ordered 2 file cabinets from Administrative Services for $30 on 10/16/2018. You may not have but I did to complete the storage of the tablets.

As for the $67,681 payment to Software House International for Dark Web Monitoring, we should allocate it to Dan's new category "J3" (Election Security Improvements) in the 2018 HAVA Funds. As you have corrected above, J8 would be the new category.

I am now ready to allocate salaries and wages, but will need Dan's new categories. They need not be fully automated, but he might have done so by the time you return from vacation – say Dec. 26.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Monday, December 17, 2018 11:04 AM
To: Nancy Swett
Cc: Daniel J Cloutier
Subject: Correction - hava expenditures July through November

Nancy,

Correction. As for the $67,681 payment to Software House International for Dark Web Monitoring, **we should allocate it to Dan's new category "J8" (Election Security Improvements) in the 2018 HAVA Funds.**

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

From: Anthony Stevens
Sent: Friday, December 14, 2018 6:24 PM
To: Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Subject: FW: hava expenditures July through November

Nancy,

See below chart for changes I made today.

Changes today are in blue background. Changes yesterday are in yellow background. Both are valid for now.

I am not sure if the two file cabinets used for AVS storage and perhaps surplused (??) to White Farm on 8/14/2018 should appear as a charge of $80 to us.

Also, I am not sure I ordered 2 file cabinets from Administrative Services for $30 on 10/16/2018.

As for the $67,681 payment to Software House International for Dark Web Monitoring, we should allocate it to Dan's new category "J3" (Election Security Improvements) in the 2018 HAVA Funds.

I am now ready to allocate salaries and wages, but will need Dan's new categories. They need not be fully automated, but he might have done so by the time you return from vacation – say Dec. 26.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

NEW HAMPSHIRE
DEPARTMENT OF STATE

William M. Gardner
Secretary of State

Robert P. Ambrose
Senior Deputy Secretary of State

David M. Scanlan
Deputy Secretary of State

Anthony B. S. Stevens
Assistant Secretary of State

July 12, 2018

Mr. Brian D. Newby
Executive Director
U.S. Election Assistance Commission
1335 East West Highway, Suite 4300
Silver Spring, MD 20910

Re: Input Plan, Narrative and Budget for the period March 23, 2018 through September 30, 2019, pursuant to the 2018 Election Reform Program payments authorized by the U.S. Congress in the Consolidated Appropriations Act of 2018, and the 5% State match.

Dear Mr. Newby:

Please find herewith New Hampshire's Input Plan, Narrative and Budget for the period March 23, 2018 through September 30, 2019 to satisfy the United States Election Assistance Commission's request for "1-3 page project narrative/budget for how the funds will be used in your state/territory."

I. Stakeholder Input Plan

Following passage of the 2018 Election Reform Program, the Secretary of State has gathered input for this plan in over 40 sessions at multiple locations throughout the State with state election officials, moderators, clerks, supervisors of the checklist, state cybersecurity officials, and individuals with disabilities.

During this time frame, the Secretary of State has conducted the following:

- Security training during the town and city clerks' regional workshops and introductory training in the statewide voter registration system;
- Interviews and listening sessions with a variety of local election officials;
- Cybersecurity assessments; and
- An attack surface assessment.

In addition, two of the Secretary of State's staff and a local election official participated in an election cybersecurity tabletop exercise conducted by the Harvard Kennedy School's Belfer Center.

In connection with the 2018 Election Reform Program adopted by Congress, the Secretary of State has:

- Identified and is working with cybersecurity companies to assess vulnerabilities and strengthen resilience;
- Assessed a number of attack surfaces;
- Tested and used cybersecurity training methodologies;
- Obtained feedback from election officials on readiness to learn, adopt, internalize, and implement cybersecurity and security practices;
- Obtained input and recommendations concerning training and election integrity issues;
- Obtained feedback on goals, best practices, and local needs toward achieving cybersecurity and resilience;
- Identified ongoing priorities and maintenance requirements to achieve goals associated with HAVA; and
- Assessed the need to improve the accessible voting system and discussed the issues involved with people with disabilities.

Based on the above stakeholder input, the Secretary of State has identified and prioritized cybersecurity needs in order to develop the following narrative and budget for Congress's anticipated 2018 Election Reform Program payment and the State's 5% match.

II. Narrative

The Secretary of State may use Congress's 2018 payments as set forth by Congress in the 2018 Election Reform Program and HAVA Section 101, as follows:

A. Enhance election technology and make election security improvements;
B. Comply with the requirements under HAVA Title III;
C. Improve the administration of elections for Federal office;
D. Educate voters concerning voting procedures, voting rights, and voting technology;
E. Train election officials, poll workers, and election volunteers;
F. Review the State's plan for any necessary modifications regarding HAVA payments;
G. Improve voting systems and technology and methods for casting and counting votes; and
H. Provide access for individuals with disabilities.

Goals

The following are New Hampshire's ongoing cybersecurity goals:

- Resilience training for election officials

- Encouraging developing of local Continuity of Operations Plans
- Operating a polling place without dependence on the electrical grid
- Conducting quick and accurate hand counting
- Effective reconciliation
- Saving/printing checklist before election day

- Cybersecurity training for election officials
  - Terms and concepts
  - Threats
  - Hacker awareness
  - Avoiding phishing, ransomware, and social engineering attacks
  - Incident and threat reporting
  - Incident response

- Leveraging existing cybersecurity programs offering free services
  - Information sharing with states and local governments

- Vulnerability assessment and remediation
  - Ongoing risk assessments
  - Insider threat analysis
  - External threat analysis
  - Penetration testing (internal and external)

- Hardening databases and servers
  - Avoiding phishing, ransomware, and social engineering attacks
  - Monitoring those who access elections databases
  - Multi-factor authentication
  - USB port analysis
  - User log analysis
  - Endpoint security – scanning emails, anti-virus
  - Visibility and analysis of all data on servers
  - Device compliance
  - Software to investigate and obtain visibility of each attack step (addressing malware, ransomware, etc.)
  - User behavioral analysis, looking for and reporting anomalies
  - Security scans 24/7/365

- State employee training and monitoring
  - Avoiding phishing, ransomware, and social engineering attacks
  - Cybersecurity courses
  - Monitoring server and email use
  - Tabletop exercises in cybersecurity resilience

- Avoiding inadvertent creation of new attack surfaces
- Automated threat response
- Actionable analysis
- Breach protection
- Compromise assessment
- On-board networking

III. Budget: $977,216 for 18 months

Based on Congress's 2018 Election Reform Program appropriation, the State anticipates receiving 2018 federal payments of $3,102,253 and a state match of $155,133, for an anticipated total of $3,257,386. The State plans to implement this plan by spending the amount of $977,216 in the 18 months between March 23, 2018 and September 30, 2019, the Federal fiscal year end. The U.S. Election Assistance Commission has indicated that, from a federal perspective, 2018 federal payments can be spent starting on March 23, 2018. This federal perspective does not preempt the need to comply with state laws.

For more than 12 years, the Secretary of State's office has sought to avoid creation of new attack surfaces and conducted regular cybersecurity and resilience training. Back-ups have been saved in multiple locations and election officials have been encouraged to save and, if necessary, print out checklists well before each election. Subject to the above Narrative, these funds will be used to build on prior efforts to enhance cybersecurity and resilience.

It would be neither prudent nor efficient at this time to define budget needs by small categories. Flexibility in using staff and/or consultants leads to better cybersecurity outcomes and posture. Cybersecurity and resilience has and continues to be integrated into procedures, training, Help Desk services, and hardware and software.

This plan, narrative and budget is intended to provide the general public and interested parties with a useful description of our plans to use the 2018 Election Reform Program payment and the 5% State match.

Sincerely yours,

William M. Gardner

CC: Mark Abbott, U.S. Election Assistance Commission

2018 HAVA ELECTION REFORM PROGRAM

Report Information — **CFDA # 90.404** — **Non-Construction Program**

Name of Organization: New Hampshire Secretary of State

Period Start: 3/23/2018

Period End: 9/30/2018

SECTION A - SUMMARY

FEDERAL & NON-FEDERAL FUNDS (Match)

BUDGET CATEGORIES	PROGRAM CATEGORIES (a) Voting Equipment	(b) Election Auditing	(c) Voter Registration Systems	(d) Cyber Security	(e) Communications	(f) Election Official Education	(g) Enhance Election Technology	TOTALS	% Fed Total
1. PERSONNEL (including fringe)				$ 16,872.11		$ 12,333.44	$ 10,458.59	$ 39,664.14	31%
2. EQUIPMENT								$ -	0%
3. SUBGRANTS- to local voting jurisdictions								$ -	0%
4. TRAINING (N/A. See Election Official Education Column)								$ -	0%
5. All OTHER COSTS				$ 80,194.00			$ 9,568.00	$ 89,762.00	69%
6. TOTAL DIRECT COSTS (1-6)	$ -			$ 97,066.11	$ -	$ 12,333.44	$ 20,026.59	$ 129,426.14	
7. INDIRECT COSTS (if applied)		$ -						$ -	0%
8. **Total Federal**	$ -	$ -	$ -	$ 97,066.11	$ -	$ 12,333.44	$ 20,026.59	$ 129,426.14	
11. Non-Federal Match								$ -	
12. Total Program	$ -	$ -	$ -	$ 97,066.11	$ -	$ 12,333.44	$ 20,026.59	$ 129,426.14	
13. Percentage By Category	0%	0%	0%	75%	0%	10%	15%		

State Match 5.0%

A. Do you have an Indirect Cost Rate Agreement approved by the Federal government or some other non-federal entity? Not applicable

If yes, please provide the following information:

B. Period Covered by the Indirect Cost Rate Agreement (mm/dd/yyyy-mm/dd/yyy):

C. Federal agency: U. S. Election Assistance Commission

D. If other than Federal agency, please specify:

E. The Indirect Cost Rate is:

NEW HAMPSHIRE
DEPARTMENT OF STATE

William M. Gardner
Secretary of State

Robert P. Ambrose
Senior Deputy Secretary of State

David M. Scanlan
Deputy Secretary of State

Anthony B.S. Stevens
Election Director

February 8, 2019

Mr. Brian D. Newby
Executive Director
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Re: Title I 2018 Election Reform Program - FFY 2018 - Analysis and Description

Dear Mr. Newby:

Please find attached the report applicable to:

(a) Title I 2018 Election Reform Program – Federal Fiscal Year 2018 – Analysis and Description of Activities Funded.

Sincerely yours,

Anthony B. S. Stevens

State House Room 204, 107 N. Main St., Concord, NH 03301
Phone: 603-271-8238 Fax: 603-271-8242
TDD Access: Relay NH 1-800-735-2964
www.sos.nh.gov email: NHVotes@sos.nh.gov

NEW HAMPSHIRE
DEPARTMENT OF STATE

William M. Gardner
Secretary of State

Robert P. Ambrose
Senior Deputy Secretary of State

David M. Scanlan
Deputy Secretary of State

Anthony B.S. Stevens
Election Director

February 6, 2019

Mr. Brian D. Newby
Executive Director
U.S. Election Assistance Commission
1335 East-West Highway, Suite 4300
Silver Spring, MD 20910

Re: State HAVA Funding Reports for FFY 2018: Title I and Title II, and Title I 2018 Election Reform Funds

Dear Mr. Newby:

Please find attached the Standard Form 425 reports applicable to:

(a) HAVA Title I, Section 101 funds for federal fiscal year 2018;
(b) HAVA Title II, Section 251 funds for federal fiscal year 2018;
(c) HAVA Title I 2018 Election Reform Funds for federal fiscal year 2018;
(d) HAVA Title I FFY 2018 analysis and description of activities funded;
(e) HAVA Title II FFY 2018 analysis and description of activities funded; and
(f) HAVA Title I 2018 Election Reform Funds Budget Worksheet.

We will submit the following shortly:

(a) Title I 2018 Election Reform Funds – analysis and description of activities funded.

Sincerely yours,

Anthony B. S. Stevens

State House Room 204, 107 N. Main St., Concord, NH 03301
Phone: 603-271-8238 Fax: 603-271-8242
TDD Access: Relay NH 1-800-735-2964
www.sos.nh.gov email: NHVotes@sos.nh.gov

Title I Spending Report

Pursuant to 42 USC 15408 (HAVA Section 258)
October 1, 2017 – September 30, 2018

The following is presented in the order and the titles used in the State Plan, with reference to the applicable category in HAVA. Total spending of Title I funds (CFDA# 39.011), exclusive of 2018 Title I Election Reform Program (CFDA# 90.404) expenditures, was $32,124.41. The categories below are referenced on pages 31-37 & 39 of the State Plan and in HAVA Title I. Purposes include improving administration of elections.

Voting Systems - Title I(b)(1)(A) $1,114.85

The Department of State used the election facilities in the State Archives and Records Building at 9 Ratification Way in Concord to inventory, program and mobilize all tablets used in the accessible voting system. The services of an Election Director, a HAVA Information Representative, a trainer/HAVA Help Desk assistant, and a Help Desk assistant were partially allocated to this account. Training for Department of State staff, including travel to conferences, is also allocated to this account. Payments were made for copier and printer supplies; temporary personnel, including clerks, their staff and supervisors of the checklist; facilitating the canvass of election results; obtaining and confirming election data to establish state primary winners for general election ballots; and checking and distributing absentee ballots in compliance with the MOVE Act.

Statewide Voter Registration System - Title I(b)(1)(A) $29,497.19

The computer training lab in the Archives and Records Building was utilized to train supervisors of the checklist, clerks and their staff to use the statewide voter registration system. The system accommodates 1232 active users, representing supervisors of the checklist and clerks in the 300 towns and city wards of the state, all of which require training periodically. New officials are elected each year and require training. The staff identified in Voting Systems above were also partially allocated to this account.

Election Official Training/Voter Education – Title I(b)(1)(C) & (D) $27.90

The Department of State assigned employees and a part-time supervisor of the checklist to work on HAVA-related tasks, including election official training and voter education. The Department of State attended NASED and NASS meetings for training.

The Department of State paid for fuel for travel to training events.

Department of State staff attended training and conventions.

The Department of State, with the help of the Attorney General, reviewed and updated on-line training for election officials.

Administrative Complaint Procedure – Title I(b)(1)(B) & (H) - 0 -

Polling Place Accessibility - Title I(b)(1)(G) - 0 -

Program Management - Title I(b)(1)(B),(E) & H) $1,484.47

The Department of State assigned employees to work on HAVA-related tasks, including program management. The Department of State purchased office equipment, office supplies, postal, telephone and fax services, vehicle upkeep, and printing.

Title II Spending Report

Pursuant to 42 USC 15408 (HAVA Section 258)
October 1, 2017 – September 30, 2018

The following is presented in the order and the titles used on page 28 of the State Plan, with reference to the applicable category in HAVA. The following figures reflect spending of both federal and state matching funds. Total Title II spending (CFDA# 90.401) amounted to $452,738.06 in Federal Fiscal Year 2018.

Title II Staff

The Department of State assigned one Assistant Secretary of State, one HAVA Information Representative, two trainer/HAVA Help Desk assistants, who devoted a portion of their time to this work. One part-time employee assisted with Help Desk and secretarial services. The Department hired supervisors of the checklist as vendors to help test ballot configuration and audio on the accessible voting system ("AVS") system.

One assistant secretary of state and one trainer/Help Desk specialist were responsible, on a part-time basis, for regional town clerk training and election law training, with input from the Attorney General's Office. One HAVA Information Representative assisted with development of on-line election law training. A part-time employee for Help Desk and secretarial services organized the training schedule and arranged handouts.

Voting System Requirements (Section 301) $47,101.17

1) The Attorney General, in coordination with the Secretary of State, sent out county sheriffs, State Police and Attorney General personnel to inspect polling places for Title III compliance on the September 11, 2018 State Primary and to report on polling place accessibility, the use of the AVS, and HAVA-compliant voter information posters. This process, conducted during September, 2018, helped document compliance with HAVA Title III.

2) The Department of State conducted an inventory check of one4all AVS equipment in the field, replacing components that were not operative.

3) Prior to the September 11, 2018 State Primary, Department of State personnel configured the one4all AVS ballot and checked the accuracy and evaluated the audio for usability.

4) The Department of State made no vendor payments under any AVS contract. (Contract with Democracy Live for the 2018 General Election was pending by September 30, 2018.

Computerized Statewide Voter Registration System (HAVA Section 303) $326,385.23

1) From October, 2017 through September, 2018, the Department of State trained in SVRS:

(a) 401 local election officials in 12 sessions of SVRS Fast and Curious (advanced) Training in late 2017 at the HAVA training facility in the Archives and Records Building.

(b) 178 local election officials in 11 sessions of SVRS Introductory Training in the Spring of 2018 at the HAVA training facility in the Archives and Records Building, relying on state trainers and using the assistance of supervisors of the checklist on a temporary basis.

2) The Department of State made payments to the SVRS vendor.

Voter Education/Election Official Training to Meet Title III Requirements $79,251.66

1) From October 1, 2017 through September 30, 2018, the Department of State trained:
(a) 262 clerks and their staff during five clerks' Regional Workshops in May - June, 2018;
(b) 25 clerks and their staff at the New Clerks training in April, 2018;
(c) 5 clerks and their staff at the clerks' certification training in August, 2018;
(d) 401 local election officials in 12 sessions of SVRS Fast and Curious (advanced) Training in late 2017 at the HAVA training facility in the Archives and Records Building.
(e) 178 local election officials in 11 sessions of SVRS Introductory ElectioNet Training in the Spring of 2018 at the HAVA training facility in the Archives and Records Building, relying on state trainers and certain supervisors of the checklist (as assistants).

2) The Department of State, with the help of the Attorney General's Office, continued to update a program begun with Pew funding to create and up-date on-line training of state election laws. This updated coverage relies on the ongoing time and effort of the Department of State and the Attorney General to maintain it and remain current with changing laws. This capability was designed to potentially reach over 5,000 election officials and poll workers with Internet connections, particularly those that cannot attend in-person election law training.

3) Department of State personnel attended HAVA-related training sessions at NASS/NASED and other conferences.

Title I (2018 Funds) Spending Report
2018 Election Reform Program
March 23, 2018 – September 30, 2018 (FFY 2018)

Pursuant to 42 USC 15408 (HAVA Section 258) - 107th Congress, Public Law 107-252 & the Consolidated Appropriations Act, 2018 – 115th Congress, Public Law 115-141

Total spending of 2018 Election Reform Program (CFDA #90.404) Title I Funds was $129,426.14 in FFY 2018. This spending was consistent with the Secretary of State's 2018 Input Plan, Narrative and Budget.

The following categories are referenced in the Secretary of State's 2018 Input Plan, Narrative and Budget covering the period March 23, 2018 through September 30, 2019, submitted to the U.S. Election Assistance Commission on July 12, 2018. This Plan set forth how the State planned to carry out and expend 2018 Election Reform Program funds authorized by the 115th U.S. Congress in the Consolidated Appropriations Act of 2018.

While considerable efforts were directed toward election technology improvements and election security before June 30, 2018, only one payment in these categories was reported in this account (CFDA #90.404) prior to the end of the State Fiscal Year on June 30, 2018. Most of the spending reported herein occurred in the final quarter of Federal Fiscal Year 2018, July 1, 2018 – September 30, 2018. Most spending directed toward election technology improvements and election security before June 30, 2018 was reflected in HAVA Title I and Title II reports and not funded with 2018 Election Reform Program funds. No spending of the State match for 2018 Election Reform Program payments is reflected in this report because State matching funds have not yet been appropriated.

The State reports HAVA expenditures on a cash basis effectively, consistent with State standards (which call for a "modified accrual" basis for State agencies). To assist readers, notes herein refer to ongoing work that in some cases would have been accounted for in the Election Fund as accrued expenses in FFY 2018 if New Hampshire's State Government were on a full accrual basis.

A. Voting Systems - Title I(b)(1)(A) -$0 –

On September 11, 2018, the Department of State rolled out a new version of the one4all accessible voting system using open source software on a new browser in order to improve the voice quality. As of September 30, 2018, the State had initiated discussions with Democracy Live to enable voters with disabilities and other one4all users to mark a pre-printed ballot at a majority of polling places in the State using the existing one4all hardware. Work on this project had been initiated, but not completed and invoiced.

E. Election Official Training/Voter Education – Title I(b)(1)(C) & (D)

Work	Detail	Amount	Subtotal
Personnel/Fringe – Election Official Education		$12,333.44	**12,333.44**
Total - Education			**12,333.44**

In FFY 2018, the Secretary of State's staff focused on achieving election official training goals aimed at resilience and cybersecurity training, as set forth in the Secretary's 2018 Plan, Narrative and Budget.

- Resilience training for election officials
  - ✓ Encouraging developing of local Continuity of Operations Plans
  - ✓ Operating a polling place without dependence on the electrical grid
  - ✓ Conducting quick and accurate hand counting
  - ✓ Effective reconciliation
  - ✓ Saving/printing checklist before election day

- Cybersecurity training for election officials
  - ✓ Terms and concepts
  - ✓ Threats
  - ✓ Hacker awareness
  - ✓ Avoiding phishing, ransomware, and social engineering attacks
  - ✓ Incident and threat reporting
  - ✓ Incident response

- State elections staff - training and monitoring
  - ✓ Avoiding phishing, ransomware, and social engineering attacks
  - ✓ Cybersecurity courses
  - ✓ Monitoring server and email use
  - ✓ Tabletop exercises in cybersecurity training

Security & Cybersecurity: Since July 1, 2018, substantial portions of the services of an Election Director, the statewide voter registration system (SVRS) subject matter expert, a HAVA Informational Representative, and one trainer/HAVA Help Desk assistant were allocated to information security. This was reflected in one hour of security focus in 2018 SVRS Introductory Training (11 sessions, 178 participants), clerks' certification training (1 session, 5 participants), training in new security concepts at the 2018 Clerks' Regional Workshops (5 sessions, 262 participants), and training in election reporting and reconciliation and security at the 2018 Summer Election Law Training (17 sessions, 1,241 participants).

Department of State staff participated in the March 27-28, 2018 Tabletop Exercises conducted by the Belfer Center at the Harvard Kennedy School in Cambridge, MA. Staff also attended the 2018 Annual Meeting of the Multi-State Information Sharing & Analysis Center (MS-ISAC) and Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC), as well as the 2018 Summer Meeting of the National Association of State Election Directors (NASED), where they received cybersecurity information and updates.

I. Enhance Election Technology

Work	Detail	Amount	Category Subtotal
Personnel/Fringe	CFDA #90.404 Election Fund ledger, July 1 – September 30, 2018	$10,458.59	**10,458.59**
SVRS: Enabling tracking of out-of-state drivers' licenses that voters presented to ballot clerks in order to obtain a ballot	104 hours X $92/hour – (from SVRS vendor invoice #026130)	$9,568.00	
All Other Costs - subtotal			**$9,568.00**
Total – Enhance Election Technology			**$20,026.59**

In FFY 2018, the Secretary of State's staff and vendors devoted substantial efforts to implement new election technology as set forth in the Secretary's 2018 Plan, Narrative and Budget, which calls for enhancing election technology.

Note: About $211,000 was committed to enhancing election technology but was not charged to this account in Federal Fiscal Year 2018:

The State had ongoing projects to enhance election technology, not included in this FFY 2018 financial report, of approximately:

- $100,000 for improvements to its election management system, which were not charged to this account due to efforts aimed at careful adherence to HAVA Section 254 (maintenance of effort) requirements;

- $14,000 to improve the death records interface in the SVRS; and

- $97,000 to enable individuals with disabilities and other one4all users to mark pre-printed ballots using existing one4all hardware in the 2018 General Election had not been invoiced – initiated in FFY 2018 and expected to be recorded as an expense in FFY 2019. Refer to A. Voting Systems - Title I(b)(1)(A) above.

J. Election Security Improvements

Work	Detail	Amount	Category Subtotal
Personnel/Fringe – election security improvements	CFDA #90.404 Election Fund ledger, July 1 – Sept. 30, 2018	$16,872.11	**$16,872.11**
Fully automate state's capacity to save to file each local checklist, ready-to-print – as a precautionary back-up in advance of an election	136 hours X $92/hour (from SVRS vendor's maintenance and support invoice # 025872)	$12,513.00	
Web monitoring, including dark web monitoring		$67,681.00	
All Other Costs - subtotal			**$80,194.00**
Total – Election Security Improvements			**$97,066.11**

During FFY 2018, the Secretary of State's staff and vendors devoted substantial efforts to achieve the following election security goals identified in the Secretary's 2018 Input Plan, Narrative and Budget:

- Vulnerability assessment and remediation
  - ✓ Ongoing risk assessments
  - ✓ Insider threat analysis
  - ✓ External threat analysis
  - ✓ Penetration testing (internal and external)

- Hardening databases and servers
  - ✓ Avoiding phishing, ransomware, and social engineering attacks
  - ✓ Monitoring those who access elections databases
  - ✓ Multi-factor authentication
  - ✓ USB port analysis
  - ✓ User log analysis
  - ✓ Endpoint security – scanning emails, anti-virus
  - ✓ Visibility and analysis of all data on servers
  - ✓ Device compliance
  - ✓ Software to investigate and obtain visibility of each attack step (addressing malware, ransomware, etc.)
  - ✓ User behavioral analysis, looking for and reporting anomalies
  - ✓ Security scans 24/7/365

- Avoiding inadvertent creation of new attack surfaces
- Automated threat response
- Actionable analysis
- Breach protection
- Compromise assessment

Note: About $270,000 in election security improvements was not charged to this account (# 90.404) in Federal Fiscal Year 2018, although these improvements had been purchased.

The State had committed to ongoing election security improvements, not included in this FFY 2018 financial report, of approximately:

- $81,000 for a software revision to implement multi-factor authentication in the statewide voter registration system – software substantially completed;

- $43,000 for software to detect and prevent execution of malware – in service, October, 2018;

- $20,000 for software to detect and prevent phishing and other hijacking attempts – in service, September, 2018;

- $63,000 for internal and external penetration testing – in service, September, 2018; and

- $63,000 for compromise assessment - in service, October 2018.

Federal Financial Report

(Follow form Instructions)

OMB Number: 4040-0014
Expiration Date: 01/31/2019

1. Federal Agency and Organizational Element to Which Report is Submitted	2. Federal Grant or Other Identifying Number Assigned by Federal Agency (To report multiple grants, use FFR Attachment)
U.S. Election Assistance Commission	Title II, 251; CFDA# 90.401

3. Recipient Organization (Name and complete address including Zip code)

Recipient Organization Name:	New Hampshire Secretary of State
Street1:	State House, Room 204
Street2:	107 North Main Street
City:	Concord
County:	
State:	NH: New Hampshire
Province:	
Country:	USA: UNITED STATES
ZIP / Postal Code:	03301

4a. DUNS Number	4b. EIN	5. Recipient Account Number or Identifying Number (To report multiple grants, use FFR Attachment)
36-185-7758	02-6000618	Title II, 251; CFDA# 90.401

6. Report Type	7. Basis of Accounting	8. Project/Grant Period		9. Reporting Period End Date
☐ Quarterly ☐ Semi-Annual ☒ Annual ☐ Final	☒ Cash ☐ Accrual	From: 05/14/2003	To: 01/01/9999	09/30/2018

10. **Transactions**	Cumulative
(Use lines a-c for single or multiple grant reporting)	
Federal Cash (To report multiple grants, also use FFR attachment):	
a. Cash Receipts	0.00
b. Cash Disbursements	0.00
c. Cash on Hand (line a minus b)	0.00
(Use lines d-o for single grant reporting)	
Federal Expenditures and Unobligated Balance:	
d. Total Federal funds authorized	13,021,803.00
e. Federal share of expenditures	10,173,178.96
f. Federal share of unliquidated obligations	0.00
g. Total Federal share (sum of lines e and f)	10,173,178.96
h. Unobligated balance of Federal Funds (line d minus g)	2,848,624.04
Recipient Share:	
i. Total recipient share required	861,806.07
j. Recipient share of expenditures	394,085.50
k. Remaining recipient share to be provided (line i minus j)	467,720.57
Program Income:	
l. Total Federal program income earned	2,292,595.34
m. Program Income expended in accordance with the deduction alternative	0.00
n. Program Income expended in accordance with the addition alternative	0.00
o. Unexpended program income (line l minus line m or line n)	2,292,595.34

11. Indirect Expense

a. Type	b. Rate	c. Period From	Period To	d. Base	e. Amount Charged	f. Federal Share
			g. Totals:			

12. Remarks: Attach any explanations deemed necessary or information required by Federal sponsoring agency in compliance with governing legislation:

Add Attachment | Delete Attachment | View Attachment

13. Certification: By signing this report, I certify to the best of my knowledge and belief that the report is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, Section 1001 and Title 31, Sections 3729-3730 and 3801-3812).

a. Name and Title of Authorized Certifying Official

Prefix: | First Name: Anthony | Middle Name: B.S.

Last Name: Stevens | Suffix:

Title: Election Director

b. Signature of Authorized Certifying Official

Anthony B. Stevens

c. Telephone (Area code, number and extension)

(603)271-8238

d. Email Address

Anthony.Stevens@sos.nh.gov

e. Date Report Submitted

02/06/2019

14. Agency use only:

Standard Form 425

Federal Financial Report

(Follow form Instructions)

OMB Number: 4040-0014
Expiration Date: 01/31/2019

1. Federal Agency and Organizational Element to Which Report is Submitted	2. Federal Grant or Other Identifying Number Assigned by Federal Agency (To report multiple grants, use FFR Attachment)
U.S. Election Assistance Commission	Title I (2018); CFDA# 90.404

3. Recipient Organization (Name and complete address including Zip code)

Recipient Organization Name: New Hampshire Secretary of State

Street1: State House, Room 204

Street2: 107 North Main Street

City: Concord County:

State: NH: New Hampshire Province:

Country: USA: UNITED STATES ZIP / Postal Code: 03301

4a. DUNS Number	4b. EIN	5. Recipient Account Number or Identifying Number (To report multiple grants, use FFR Attachment)
36-185-7758	02-6000618	Title I (2018); CFDA# 90.404

6. Report Type	7. Basis of Accounting	8. Project/Grant Period		9. Reporting Period End Date
☐ Quarterly ☐ Semi-Annual ☒ Annual ☐ Final	☒ Cash ☐ Accrual	From: 05/14/2003	To: 01/01/9999	09/30/2018

10. **Transactions**	Cumulative
(Use lines a-c for single or multiple grant reporting)	
Federal Cash (To report multiple grants, also use FFR attachment):	
a. Cash Receipts	0.00
b. Cash Disbursements	0.00
c. Cash on Hand (line a minus b)	0.00
(Use lines d-o for single grant reporting)	
Federal Expenditures and Unobligated Balance:	
d. Total Federal funds authorized	3,102,253.00
e. Federal share of expenditures	129,426.14
f. Federal share of unliquidated obligations	0.00
g. Total Federal share (sum of lines e and f)	129,426.14
h. Unobligated balance of Federal Funds (line d minus g)	2,972,826.86
Recipient Share:	
i. Total recipient share required	0.00
j. Recipient share of expenditures	0.00
k. Remaining recipient share to be provided (line i minus j)	0.00
Program Income:	
l. Total Federal program income earned	643.49
m. Program Income expended in accordance with the deduction alternative	0.00
n. Program Income expended in accordance with the addition alternative	0.00
o. Unexpended program income (line l minus line m or line n)	643.49

11. Indirect Expense

a. Type	b. Rate	c. Period From	Period To	d. Base	e. Amount Charged	f. Federal Share
			g. Totals:			

12. Remarks: Attach any explanations deemed necessary or information required by Federal sponsoring agency in compliance with governing legislation:

Add Attachment | Delete Attachment | View Attachment

13. Certification: By signing this report, I certify to the best of my knowledge and belief that the report is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, Section 1001 and Title 31, Sections 3729-3730 and 3801-3812).

a. Name and Title of Authorized Certifying Official

Prefix: | First Name: Anthony | Middle Name: B.S.

Last Name: Stevens | Suffix:

Title: Election Director

b. Signature of Authorized Certifying Official

c. Telephone (Area code, number and extension): (603)271-8238

d. Email Address: Anthony.Stevens@sos.nh.gov

e. Date Report Submitted: 02/06/2019

14. Agency use only:

Standard Form 425

Federal Financial Report

(Follow form Instructions)

OMB Number: 4040-0014
Expiration Date: 01/31/2019

1. Federal Agency and Organizational Element to Which Report is Submitted	2. Federal Grant or Other Identifying Number Assigned by Federal Agency (To report multiple grants, use FFR Attachment)
U.S. Election Assistance Commission	Title I, 101: CFDA# 39.011

3. Recipient Organization (Name and complete address including Zip code)

Recipient Organization Name: New Hampshire Secretary of State

Street1: State House, Room 204

Street2: 107 North Main Street

City: Concord County:

State: NH: New Hampshire Province:

Country: USA: UNITED STATES ZIP / Postal Code: 03301

4a. DUNS Number	4b. EIN	5. Recipient Account Number or Identifying Number (To report multiple grants, use FFR Attachment)
36-185-7758	02-6000618	Title I, 101; CFDA# 39.011

6. Report Type	7. Basis of Accounting	8. Project/Grant Period		9. Reporting Period End Date
☐ Quarterly ☐ Semi-Annual ☒ Annual ☐ Final	☒ Cash ☐ Accrual	From: 05/14/2003	To: 01/01/9999	09/30/2018

10. **Transactions**	Cumulative
(Use lines a-c for single or multiple grant reporting)	
Federal Cash (To report multiple grants, also use FFR attachment):	
a. Cash Receipts	0.00
b. Cash Disbursements	0.00
c. Cash on Hand (line a minus b)	0.00
(Use lines d-o for single grant reporting)	
Federal Expenditures and Unobligated Balance:	
d. Total Federal funds authorized	5,000,000.00
e. Federal share of expenditures	2,460,199.61
f. Federal share of unliquidated obligations	0.00
g. Total Federal share (sum of lines e and f)	2,460,199.61
h. Unobligated balance of Federal Funds (line d minus g)	2,539,800.39
Recipient Share:	
i. Total recipient share required	0.00
j. Recipient share of expenditures	0.00
k. Remaining recipient share to be provided (line i minus j)	0.00
Program Income:	
l. Total Federal program income earned	1,193,152.62
m. Program Income expended in accordance with the deduction alternative	0.00
n. Program Income expended in accordance with the addition alternative	0.00
o. Unexpended program income (line l minus line m or line n)	1,193,152.62

11. Indirect Expense

a. Type	b. Rate	c. Period From	Period To	d. Base	e. Amount Charged	f. Federal Share
			g. Totals:			

12. Remarks: Attach any explanations deemed necessary or information required by Federal sponsoring agency in compliance with governing legislation:

Add Attachment | Delete Attachment | View Attachment

13. Certification: By signing this report, I certify to the best of my knowledge and belief that the report is true, complete, and accurate, and the expenditures, disbursements and cash receipts are for the purposes and objectives set forth in the terms and conditions of the Federal award. I am aware that any false, fictitious, or fraudulent information, or the omission of any material fact, may subject me to criminal, civil or administrative penalties for fraud, false statements, false claims or otherwise. (U.S. Code Title 18, Section 1001 and Title 31, Sections 3729-3730 and 3801-3812).

a. Name and Title of Authorized Certifying Official

Prefix: | First Name: Anthony | Middle Name: B.S.

Last Name: Stevens | Suffix:

Title: Election Director

b. Signature of Authorized Certifying Official

c. Telephone (Area code, number and extension): (603)271-8238

d. Email Address: Anthony.Stevens@sos.nh.gov

e. Date Report Submitted: 02/06/2019

14. Agency use only:

Standard Form 425

Daniel J Cloutier

From: Daniel J Cloutier
Sent: Wednesday, June 12, 2019 2:32 PM
To: Nancy Swett; Anthony Stevens
Cc: David Scanlan; Paula Penney; Orville Fitch
Subject: RE: Election Related Cybersecurity Bills - Funding Sources

I have confirmed your math and informed Anthony of this expected result of the invoices that have been delivered to you yesterday. Thank you for the chart below as that will become invaluable when the SF425 and accompanying documentation will be prepared.

Thanks,
Dan
Daniel J Cloutier

From: Nancy Swett <Nancy.Swett@SOS.NH.GOV>
Sent: Wednesday, June 12, 2019 2:30 PM
To: Anthony Stevens <Anthony.Stevens@SOS.NH.GOV>; Daniel J Cloutier <Daniel.Cloutier@sos.nh.gov>
Cc: David Scanlan <David.Scanlan@SOS.NH.GOV>; Paula Penney <Paula.Penney@SOS.NH.GOV>; Orville Fitch <Orville.Fitch@sos.nh.gov>
Subject: RE: Election Related Cybersecurity Bills - Funding Sources

Anthony,

The $155,113 match has been expended from the Corporation Division. Details of the expenditures are shown below. Additional cyber security related invoices will be paid from HAVA funds.

VENDOR#	VENDOR	INVOICE #	AMOUNT	DIVISION	INVOICE DATE	COMMENTS
273554	NUHARBOR SECURITY	NHSOS0718-02	$19,687.50	1065	7/10/2018	PROOF PRINT EMAIL
273554	NUHARBOR SECURITY	NHSOS0718-01	$9,000.00	1065	7/9/2018	SPLUNK BASE CONFIGURATION
273554	NUHARBOR SECURITY	NHSOS0718-03	$43,234.50	1065	7/24/2018	CROWDSTRIKE
175141	SOFTWARE HOUSE INTERNATIONAL	B09617871	$30,500.00	1065	3/5/2019	INTERNAL/EXTERNAL PEN TEST
175141	SOFTWARE HOUSE INTERNATIONAL	B09483704	43685.53	1065	2/6/2019	CS CONSULTING HOUR – 101 HOURS
175141	SOFTWARE HOUSE INTERNATIONAL	B09336051	9005.47	1065	1/4/19	50% INTERNAL/EXTERNAL PEN TEST (FULL INVOICE AMOUNT $30,500, $9005.47 PAID FROM 1065 AND $21,494.53 PAID FROM 1064)

Thanks,

Nancy Swett

Office of the Secretary of State
603-271-3242 phone
603-271-6316 fax

From: Anthony Stevens
Sent: Tuesday, May 21, 2019 5:10 PM
To: Nancy Swett; Daniel J Cloutier
Cc: David Scanlan; Paula Penney; Orville Fitch
Subject: Election Related Cybersecurity Bills - Funding Sources

Nancy and Dan,

Please use this communication as your instructions to use Corporation Division information technology funds to pay election-related bills incurred in Federal Fiscal Year 2019 for cybersecurity services from Falcon/Crowdstrike, Proofpoint, Fireeye/Groupsense, and Splunk, as well as election-related bills for penetration testing and compromise assessment services, until the total amount of such payments reaches $155,113. When this threshold is attained, these expenditures will constitute the required state match for the 2018 Election Reform Program funds provided by Congress, and we should record these payments and enable federal reporting accordingly. After this threshold has been reached, please charge subsequent election-related cybersecurity bills to the Election Fund.

To the extent possible, please execute this before the 2019 State Fiscal Year-end, and advise me when the above threshold for the state match has been reached, with a status report on June 20, 2019 in any event. Thank you.

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Nancy Swett
Sent: Wednesday, June 12, 2019 2:30 PM
To: Anthony Stevens; Daniel J Cloutier
Cc: David Scanlan; Paula Penney; Orville Fitch
Subject: RE: Election Related Cybersecurity Bills - Funding Sources

Anthony,

The $155,113 match has been expended from the Corporation Division. Details of the expenditures are shown below. Additional cyber security related invoices will be paid from HAVA funds.

VENDOR#	VENDOR	INVOICE #	AMOUNT	DIVISION	INVOICE DATE	CO
273554	NUHARBOR SECURITY	NHSOS0718-02	$19,687.50	1065	7/10/2018	PRO
273554	NUHARBOR SECURITY	NHSOS0718-01	$9,000.00	1065	7/9/2018	SPL
273554	NUHARBOR SECURITY	NHSOS0718-03	$43,234.50	1065	7/24/2018	CRO
175141	SOFTWARE HOUSE INTERNATIONAL	B09617871	$30,500.00	1065	3/5/2019	INT
175141	SOFTWARE HOUSE INTERNATIONAL	B09483704	43685.53	1065	2/6/2019	CS
175141	SOFTWARE HOUSE INTERNATIONAL	B09336051	9005.47	1065	1/4/19	50% AM $21

Thanks,

Nancy Swett
Office of the Secretary of State
603-271-3242 phone
603-271-6316 fax

From: Anthony Stevens
Sent: Tuesday, May 21, 2019 5:10 PM
To: Nancy Swett; Daniel J Cloutier
Cc: David Scanlan; Paula Penney; Orville Fitch
Subject: Election Related Cybersecurity Bills - Funding Sources

Nancy and Dan,

Please use this communication as your instructions to use Corporation Division information technology funds to pay election-related bills incurred in Federal Fiscal Year 2019 for cybersecurity services from Falcon/Crowdstrike, Proofpoint, Fireeye/Groupsense, and Splunk, as well as election-related bills for penetration testing and compromise assessment services, until the total amount of such payments reaches

$155,113. When this threshold is attained, these expenditures will constitute the required state match for the 2018 Election Reform Program funds provided by Congress, and we should record these payments and enable federal reporting accordingly. After this threshold has been reached, please charge subsequent election-related cybersecurity bills to the Election Fund.

To the extent possible, please execute this before the 2019 State Fiscal Year-end, and advise me when the above threshold for the state match has been reached, with a status report on June 20, 2019 in any event. Thank you.

Anthony Stevens
Election Director, Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Friday, February 8, 2019 12:47 PM
To: Brian Newby
Cc: Mark Abbott; Peg Rosenberry; David Scanlan
Subject: NH - Title I 2018 Election Reform Program Report
Attachments: NH - Title I 2018 Election Reform Program Report FFY 2018.pdf; Cover letter for Title I 2018 Report, sent February 8, 2019.pdf

Brian,

Please find attached our Title I 2018 Election Reform Program Report for FFY 2018 - Analysis and Description of Activities Funded.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From:	Anthony Stevens
Sent:	Wednesday, February 6, 2019 7:06 PM
To:	Brian Newby
Cc:	Mark Abbott; Peg Rosenberry
Subject:	NH - FFY 2018 HAVA Financial Reports
Attachments:	NH -Title I - FFY 2018 - 425.pdf; NH -Title I (2018 Funds) - FFY 2018 - 425.pdf; NH - HAVA - Title I Spending Report FFY 2018.pdf; NH - Cover letter for 2018 reports, sent February 6, 2019.pdf; NH - HAVA - Title II Spending Report FFY 2018.pdf; New Hampshire_ES_Budget_Worksheet.pdf; NH - Title II - FFY 2018 - 425.pdf

Brian,

Please find attached our FFY 2018 HAVA Financial Reports. We will send the analysis and description of activities supported by 2018 Election Reform Program Funds shortly. Thank you for your patience.

Anthony Stevens
Assistant Secretary of State
Election Director
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Daniel J Cloutier

From: Anthony Stevens
Sent: Wednesday, January 30, 2019 1:02 PM
To: David Scanlan; Daniel J Cloutier
Subject: EAC Report on Spending of 2018 Funds
Attachments: 2018 - 2019 Plan, Budget and Narrative.pdf; AS Copy of Sample_ES_Budget_Worksheet.xlsx; 2018 Funds - Title I Spending Report 2019 v3.doc

Dave and Dan,

Please take a look at this draft report to the EAC applicable to the 2018 funds appropriated by Congress. This report is expected to be finalized and submitted, along with reports for Title I and Title II HAVA expenditures, by late tomorrow. (By Friday morning, we must submit the massive EAVS data sets, so that would be too late.) For lots of sound accounting reasons, this FFY 2018 report reflects activity substantially in the final quarter of the 2018 Federal Fiscal Year, July 1, 2018 - September 30, 2018. Thanks to Dan for completing the FFY 2018 expenditures.

Secretary Gardner's 2018 Plan, Narrative and Budget (attached), submitted by us on July 12, 2018, called for $977,216 in spending through September 30, **2019**. The actual spending from this account through September 30, **2018** amounted to $129,426.14 – 13% of what was in the plan for the 18 month period in the Plan. Arguably, about 6 months out of 18 months (33%) would have run by September 30, 2018.

The notes herein refer to additional projects amounting to about $211,000 for Enhancing Election Technology and $153,000 for Election Security Improvements, totaling $364,000 in ongoing election-related work as of September 30, 2018.

So, by September 30, 2018, there about $493,000 ($129,000 actual + $364,000 pending) in election-related work completed or soon to be completed that would either enhance election technology or make election security improvements. That would be 50% of the nearly $1 million in our 18-month 2018 Narrative and Budget. (Not all will be charged to CFDA Account #90.404.)

The EAC has suggested that states report 2018 Election Reform Program spending on an accrual basis, in order to reflect ongoing work better than the modified accrual basis that New Hampshire (and probably many other states) rely on. We are sticking to the state standard of modified accrual, but try to provide additional information that might be useful for those in the general public and Congress who are interested. Dan may wish to modify the text in yellow highlights that describes the accounting method the State uses.

I would like to go over these figures with you as soon as possible. This is only a draft; suggested changes are welcome. There are other ways to present this information.

Anthony Stevens
Assistant Secretary of State
9 Ratification Way
Concord
New Hampshire 03301
Tel: (603)271-8238

Election Security and the 2016 Voter Experience

BY NATALIE ADONA AND PAUL GRONKE | DECEMBER 2, 2016

The 2016 election was one of the most hard fought and divisive in recent memory. The Democracy Fund continues to be troubled by some of the rhetoric regarding the "hacking" and "rigging" of the American election system, two topics that animated so much discussion from across the ideological spectrum this cycle. We believe the long-term impact of these messages undermines the legitimacy of the election system and further erodes public trust in our political system.

Our new infographic is based on a national survey of voters after the 2016 election that was designed to provide the Democracy Fund a snapshot of public opinion about our election system and the possible effect of the rhetoric around election fraud. This data demonstrates that while most voters had a pleasant voting experience, deep concerns exist about the integrity of American elections.

Most Americans had a pleasant voting experience and expressed confidence in the outcome.

Let's start with the good news: most Americans had a pleasant voting experience. When asked, 85.3 percent of voters said the best description of their voting experience was that it was "pleasant." This is consistent with other surveys that capture voter opinions about election administration. For example, the Cooperative Congressional Election Study (CCES) has found the majority of in person voters report having "excellent" or "good" interactions with poll workers and are generally confident that their own ballots were counted as intended. Results from the CCES also indicate that a majority people think that election officials are fair most of the time.[1]

Because public opinion about elections can be influenced by one's political associations and candidate preferences, we broke down these results by party identification. It turned out that party differences were minimal. The percentage of Republicans who reported a pleasant experience (89) was higher than among Independents (83.6) and Democrats (82.5). Still, 4 out of 5 voters who cast a ballot for Hillary Clinton reported a pleasant voting experience.

Overall, these results show that election officials ensured not only that voters can participate in the political process, but also that voters can feel good about participating. To anyone who has ever worked in an election office, this is very encouraging. A positive voter experience is never guaranteed—it has to be earned. A significant portion of the report from the Presidential Commission on Election Administration (PCEA) focused on the positive benefits that would accrue from a "customer service" orientation. A great level of detail and care is required to successfully administer an election and we want to take a moment to recognize and appreciate the hard work of election officials.

Many are concerned about voter fraud in national elections.

But let's not get too far ahead of ourselves – just because most voters walked away feeling good doesn't mean that there isn't more work to be done. Hearing claims that the election could be "rigged" or that other countries might "hack" the American election system may have heightened concerns about voter fraud. Even though there is virtually no evidence that voter fraud occurs at a scale large enough to sway electoral outcomes, confidence in vote counts decreases significantly the further removed the vote total is from the local jurisdiction. Survey data has consistently shown that respondents are less confident in state- and national-level ballot counts than in local counts.[2]

Lower confidence in national-level outcomes may make the public vulnerable to claims that the election system is "rigged" or that results could be "hacked." As shown in the infographic, 39 percent of voters were "very" or "somewhat" concerned that an electronic security breach or hack impacted national vote counts. A slightly lower but significant percentage of voters (38) had similar concerns around parties and candidates changing election results to create false or inaccurate totals. Of that group, 35 percent of Trump voters and 40 percent of Clinton voters answered that they were "very" or "somewhat" concerned that the parties or candidates changed election results.

Minority communities and younger voters were more likely to report problems and distrust with voting.

Other concerns emerged from our survey. Twenty-three percent of African Americans and 18 percent of Hispanics said that they felt fearful or intimidated voting, or had problems voting, compared to 12 percent of white voters. More than half of Hispanic respondents and 58 percent of African Americans expressed answered they were "very" or "somewhat" concerned that an electronic security breach or hack impacted vote counts, compared to 32 percent of white voters. Hispanics and African Americans were also more likely than whites to answer that they were "very" or "somewhat" concerned that a candidate or party changed the election results to create false or inaccurate vote counts.

The data revealed that age may also shape opinions about fraud. Twice as many younger respondents were "very" or "somewhat" concerned that a candidate or party changed the election results (49 percent compared to 24 percent of respondents 55 and over). It turns out that this pattern is nearly linear across smaller age cohorts, across all items, something we hope to explore in the future.

In one respect, it is encouraging that older voters, who presumably have more experience with voting, are more confident. But this also implies that younger and less experienced voters may be especially susceptible to claims about election fraud, and this could dissuade them from voting. To take just one example, we discovered that 17 percent of respondents under 55 reported that they felt fearful or intimidated, or had problems voting, compared to just 11 percent of respondents 55 years and older.

Distrust in the election system is unhealthy, and it's notable that younger and minority voters overall were more likely to report fear and intimidation while voting and were more likely to express concern about election integrity. Given the sometimes brutal tone of the campaigns this election cycle, we felt it was important to highlight these data points as worthy of further examination.

Building Trust in Elections

Despite fears around voter fraud, polling place security, and calls for an increased number of poll watchers from the campaigns, local election officials successfully served the voting public. As we look through our data, we are very encouraged by evidence that voters are more likely to think the outcome was fair when educated about key security features. Our survey data confirm

that independence, transparency, integrity, competence, and fairness translate into higher levels of public approval of the elections system.

Election officials, advocates, and others should think about how they talk about election security with voters and look for opportunities to foster trust in the system. Our data shows a need for increased voter education in three important ways:

- First, the fact that certain minorities were more likely to report some kind of problem with voting should raise concerns about election conduct and hopefully will lead to meaningful ways for election officials and others to address problems in particular communities.
- Second, because younger voters were also more likely to express concerns about election security and are probably less experienced in voting, election officials and advocates should focus their educational efforts on younger voters as well.
- Third, voters from both sides of the political aisle have concerns about election fraud and are receptive to the information and rhetoric that they hear about election processes, which opens up an opportunity for election officials to show voters how their offices address these concerns.

We will continue to explore our data and are looking forward to sharing our findings as they emerge. One of our takeaways from this survey is that, even with all the good work that's been done, voters need our help to understand election security and integrity and will listen when they're given correct information. We hope that these survey results will trigger productive conversations between voters, election officials, advocates, and others about the processes currently in place that keep elections secure.

★★★

ABOUT THE AUTHORS

Natalie Adona is the Senior Research and Learning Associate for the Elections Program at the Democracy Fund, a bipartisan foundation working to ensure that our political system is able to withstand new challenges and deliver on its promise to the American people. Focusing on a modern, trusted, voter-centric elections system, Natalie supports the Elections Program in their mission to ensure that the views and votes of citizens comes first in our democracy.

Paul Gronke is a professor of political science at Reed College and serves as an academic consultant to the Democracy Fund's Elections Program. He is also the Director of the Early Voting Information Center in Portland, Oregon.

For more information, please visit http://www.democracyfund.org/.

ENDNOTES

[1] The Cooperative Congressional Election Study has been administered in each federal election since 2006. The data are available at http://projects.iq.harvard.edu/cces/home.

[2] Michael W. Sances and Charles Stewart III. "Partisanship and Confidence in the Vote Count: Evidence from U.S. National Elections since 2000." *Electoral Studies* 40 (December 2015): 176–88. doi:10.1016/j.electstud.2015.08.004.

3rd Annual Democracy Fund / NASS Breakfast

Dr. Joseph Lorenzo Hall is the Chief Technologist and Director of the Internet Architecture project at the Center for Democracy & Technology, a Washington, DC-based non-profit advocacy organization dedicated to ensuring digital rights and that the internet remains open, innovative and free. Hall's work focuses on the intersection of technology, law, and policy, working to ensure that technical considerations are appropriately embedded into legal and policy instruments. Supporting work across all of CDT's programmatic areas, Hall provides substantive technical expertise to CDT's programs, and interfaces externally with CDT supporters, stakeholders, academics, and technologists. Hall leads CDT's Internet Architecture project, which focuses on embedding human rights values into core internet standards and infrastructure, engaging technologists in policy work, producing accessible technical material for policymakers, and specific lines of work associated with reducing chilling effects to security research and the cybersecurity of voting technologies.

Prior to joining CDT in 2012, Hall was a postdoctoral research fellow with Helen Nissenbaum at New York University, Ed Felten at Princeton University and Deirdre Mulligan at University of California, Berkeley. Hall received his Ph.D. in information systems from the UC Berkeley School of Information in 2008. His Ph.D. thesis used electronic voting as a critical case study in digital government transparency. In his postdoctoral work, he worked on implementing risk-limiting audits for digital elections, developing techniques to increase the efficiency and usability of accountability mechanisms in election auditing. Hall holds master's degrees in astrophysics and information systems from UC Berkeley and was a founding member of the National Science Foundation's ACCURATE Center (A Center for Correct, Usable, Reliable, Auditable and Transparent Elections). He has served as an expert on independent teams invited by the States of California, Ohio and Maryland to analyze legal, privacy, security, usability and economic aspects of voting systems. Hall is the Vice-Chairman of the Board of Directors of the California Voter Foundation, a member of the Board of Directors of the Verified Voting Foundation and a member of technical advisory boards to the Electronic Registration Information Center and Los Angeles County's Voting System Assessment Project. In 2012, Hall received the John Gideon Memorial Award from the Election Verification Network for contributions to election verification. In 2017, Hall was part of a team that received the Researcher Award at the 2017 O'Reilly Security Defender Awards in recognition of the team's dedication and innovative contributions to election security for organizing the first Voting Machine Hacking Village at DEFCON 25.

Sabra Horne is the Director of Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) within the National Protection and Programs Directorate Office of Cybersecurity and Communications at the Department of Homeland Security (DHS). She leads the DHS Election Task Force and agency efforts for effective partnering with the private sector, as well as state, local, tribal and territorial entities.

Prior to this role, she served at the National Security Agency (NSA) as the Deputy Chief for Information Sharing and Collaboration, facilitating the sharing of NSA's most highly classified intelligence. She was Senior Advisor to MSA Threat Operation Center leadership and led their effort to share unclassified cyber threat information with other government agencies and the private sector. She began her NSA service as a core member in the standup of the Media Leaks Task Force, which led the agency response to the public leaks of classified information in June 2013.

Ms. Horne was previously Director of Communications at the Department of Justice Office of Justice Programs, responsible for all legislative, public, and intergovernmental affairs. She began her government career at the Office of the Director of National Intelligence (ODNI) as Senior Advisor for Strategic Partnerships for Open Source, driving collaboration across the sixteen intelligence agencies in their use of open source intelligence. While at the ODNI, she also served as the Chief of Staff in the

standup of the National Maritime Intelligence Center and lead development of the Unified Intelligence Strategy for the National Intelligence Manager for Cyber, unifying intelligence collection and analysis across ten agencies. She was also detailed to DHS to support the Assistant Secretary for Infrastructure Protection in increasing information flow to the private sector.

Prior to her government service, she had an 18-year career in academic publishing, the last 12 as Senior Executive Editor for the largest list of academic criminal justice publications at Wadsworth Publishing. Ms. Horne has a Masters in Public Administration from the Harvard Kennedy School of Government.

Dr. Mike Garcia is an economist and cybersecurity expert. He is currently leading an elections best practices effort with the Center for Internet Security. The *Handbook for Elections Infrastructure Security* is a guide for all those involved in elections, from officials to information technology security staff to vendors and contracted support. It provides an overview of cybersecurity risk in elections systems and best practices to mitigate those risks.

Prior to this work, Mike led NIST's Trusted Identities Group. By focusing on market-based solutions for identity management and establishing guidelines and standards to accelerate government and commercial adoption, Mike oversaw major advances in the development and deployment of privacy-enhancing, secure, interoperable, and easy-to-use digital identity solutions. Mike had been with NIST since 2011 after serving as Sr. Cybersecurity Strategist at the Department of Homeland Security from 2009 to 2011.

Mike has a background in analytic modeling and has been an instructor of agribusiness management at Ohio State, a modeling lead for an analytics firm, a marketing research manager, and developed combat search and rescue navigation control systems for a U.S. Air Force contractor.

Mike holds a doctorate in Agricultural, Environmental, and Development Economics from Ohio State with foci in Information Security Economics and Resource Economics. Additionally, Mike holds an M.A. in Economics and an MBA from The Ohio State University, as well as a B.A. in Economics, B.S. in Computer Science, and B.S.Ed. in Education from the University of Dayton. He is a native of Cleveland, Ohio, and enjoys running, reading, and traveling.

Walter Tong, CISSP Walter consults with state agencies on a number of topics including enterprise policies, security program development and evaluations, and risk management.

He is currently involved with Georgia Center for Innovation and Training as an advisor and contributor for planning. He has developed and implemented a cyber intelligence program to provide actionable cyber intelligence products to key decision makers as part of the State Homeland Security Cyber Preparedness Program to support the state's responsibility in cyber event management and response.

Walter has held a variety of positions at GTA. He has been the Director of Enterprise Information Security, a Senior Security Advisor, and Manager of the GTA IT Security Threat Management Center. He has also served as the Information Security Officer for the Georgia Dept. of Education and Co-chair of the Critical Systems Sub-committee for the 2004 G8 Economic Summit.

As Director of Enterprise Information Security, he was responsible for implementing a risk management approach towards IT security and ensuring the integration of information security into IT projects. He has also lead the initiative to establish state-wide hiring standards for agency information security officers.

Walter's collective experience in leading many of the State's information security efforts has been instrumental in raising the awareness, management, administration and security posture for Georgia.

Hon. Denise W. Merrill was elected to her second term as Connecticut's 73rd Secretary of the State on November 4, 2014. As Connecticut's chief elections official and business registrar, Merrill has focused on modernizing Connecticut's elections, business services and improving access to public records. Secretary Merrill is focused on both civic engagement and fostering business enterprise. Since taking office, she has supported and expanded democratic participation, ensuring that every citizen's rights and privileges are protected and that every vote is counted accurately. Secretary Merrill has worked to expand voter participation through Election Day and online voter registration. She has also improved Connecticut's democratic accountability and integrity with a series of rapid response processes to Election Day problems. She was elected president of the National Association of Secretaries of State for the 2016-17 term and serves on the Board of Advisors to the U.S. Election Assistance Commission. As Connecticut's business registrar, Secretary Merrill has made it easier for businesses to interact with the office by increasing online functionality, improving response times and connecting businesses with government resources. Merrill has partnered with the U.S. Department of Commerce Export Assistance Center, the General Services Administration, and Small Business Development Administration to distribute information about business assistance and educational events being offered by these agencies. Secretary Merrill also launched an award-winning online business startup tool to help entrepreneurs navigate through various state and federal agencies. She also led the development of Connecticut's e-Regulations System, an online platform that provides access to all agency regulation-making records with real-times updates.

Prior to her election as Secretary of the State, Denise Merrill served as State Representative from the 54th General Assembly District for 17 years, representing the towns of Mansfield and Chaplin. First elected to the General Assembly in 1994, Merrill rose to the rank of House Majority Leader from 2009-2011. She also served as the House Chair of the budget writing Appropriations Committee from 2005-2009, as vice-chair of the Education Committee from 1994-1999 and as a member of the Government Administration and Elections Committee from 1995-1997. In a 2009 poll done by Connecticut magazine, Majority Leader Merrill was named by her colleagues in the legislature as "Most Respected by the Other Side of the Aisle" and "Most Effective Legislator."

Secretary Merrill is a graduate of the University of Connecticut, is licensed to practice law in the state of California, and is a classically trained pianist. She lives in Hartford. Her family includes husband Dr. Stephen Leach and his two sons, her three grown children and five grandchildren.

Center for American Progress

DEMOCRACY AND GOVERNMENT

Election Security in All 50 States

Defending America's Elections

By Danielle Root, Liz Kennedy, Michael Sozan, and Jerry Parshall Posted on February 12, 2018, 12:01 am

Getty/Katherine Frey

A woman casts her ballot at Hillsboro Old Stone School in Purcellivlle, Virginia, November 2017.

OVERVIEW

urgency for appropriate solutions and arm stakeholders with information to demand increased security measures.

PRESS CONTACT

See: Matrix of state grades

Introduction and summary

In 2016, America's elections were targeted by a foreign nation-state intent on infiltrating and manipulating our electoral system. On September 22, 2017, it was reported that the U.S. Department of Homeland Security (DHS) notified 21 states that were targeted by hackers during the 2016 election.[1] Among those states notified by DHS were: Alabama, Alaska, Colorado, Connecticut, Delaware, Florida, Illinois, Maryland, Minnesota, Ohio, Oklahoma, Oregon, North Dakota, Pennsylvania, Virginia, and Washington.[2] Arizona, California, Iowa, Texas, and Wisconsin were also among those states originally contacted by DHS. However, those states have denied that their election systems were attacked.[3] Ultimately, hackers only reportedly succeeded in breaching the voter registration system of one state: Illinois.[4] And while DHS did not name those responsible for the attempted hacks, many believe the culprits can be traced back to Russia.[5] Experts have warned that a future attack on our election infrastructure, by Russia or other malicious actors, is all but guaranteed.[6]

By now, the American people have been alerted to many vulnerabilities in the country's election systems, including the relative ease of voting machine hacking,[7] threats to voter registration systems and voter privacy,[8] and disinformation campaigns waged by foreign nation-states aimed at confusing voters and inciting conflict.[9] If left unaddressed, these vulnerabilities threaten to undermine the stability of our democratic system.

choices about the country's future—what policies will be enacted and who will represent their interests in the states, Congress, and beyond. The right of Americans to choose their own political destiny is in danger of being overtaken by foreign nation-states bent on shifting the balance of power in their favor and undermining American's confidence in election results. In our democracy, every vote counts, as evidenced by the race for Virginia's House of Delegate's 94th District, which was decided by lottery after being tied.[10] That contest illustrates the inherent worth and power behind each vote as well as the necessity of protecting elections from tampering on even the smallest scale.[11] Every vote must count, and every vote must be counted as cast.

Election security is not a partisan issue. As aptly noted by the chairman of the U.S. Senate Select Committee on Intelligence, Sen. Richard Burr (R-NC), "Russian activities during the 2016 election may have been aimed at one party's candidate, but ... in 2018 and 2020, it could be aimed at anyone, at home or abroad."[12] Failing to address existing vulnerabilities and prepare for future attacks puts the nation's security at risk and is an affront to the rights and freedoms at the core of American democracy. Already, we are running out of time to prepare for the 2018 elections, while the 2020 presidential election is looming.[13] Another attack on our elections by nation-states such as Russia is fast approaching.[14] Leaders at every level must take immediate steps to secure elections by investing in election infrastructure and protocols that help prevent hacking and machine malfunction. In doing so, the United States will be well positioned to outsmart those seeking to undermine American elections and to protect the integrity of every vote.

To understand risks to our election systems and plan for the future, it is necessary to identify existing vulnerabilities in election infrastructure so we can properly assess where resources should be allocated and establish preventative measures and strategies. Only through understanding the terrain can the nation rise to the challenge of preventing voting machine malfunction and defending America's elections from adversarial attempts to undermine our election infrastructure.

In August 2017, the Center for American Progress released a report entitled "9 Solutions for Securing America's Elections," laying out nine vulnerabilities in election infrastructure and solutions to help improve election security in time for the 2018 and 2020 elections.[15] This report builds on that analysis to provide an overview of election security and preparedness in each state, looking specifically at state requirements and practices related to:

2. Voter-verified paper ballots
3. Post-election audits that test election results
4. Ballot accounting and reconciliation
5. Return of voted paper absentee ballots
6. Voting machine certification requirements
7. Pre-election logic and accuracy testing

This report provides an overview of state compliance with baseline standards to protect their elections from hacking and machine malfunction. Some experts may contend that additional standards, beyond those mentioned here, should be required of states to improve election security. The chief purpose of this report is to provide information on how states are faring in meeting even the minimum standards necessary to help secure their elections.

It is important to note at the outset that this report is not meant to be comprehensive of all practices that touch on issues of election security. We recognize that local jurisdictions sometimes have different or supplemental requirements and procedures from those required by the state. However, this report only considers state requirements reflected in statutes and regulations and does not include the more granular—and voluminous—information on more localized practices. Furthermore, this report does not address specific information technology (IT) requirements for voting machine hardware, software, or the design of pre-election testing ballots and system programming. And while we consider some minimum cybersecurity best practices, we do not analyze specific cyberinfrastructure or system programming requirements. These technical standards and protocols deserve analysis by computer scientists and IT professionals[16] who have the necessary expertise to adequately assess the sufficiency of state requirements in those specialized areas.[17]

This report is not an indictment of state and local election officials. Indeed, many of the procedures and requirements considered and contained within this report are created by statute and under the purview of state legislators instead of election officials. Election officials are tasked with protecting our elections, are the first to respond to problems on Election Day, and work diligently to defend the security of elections with the resources available to them. Unfortunately, funding,

election security. We hope that by identifying potential threats to existing state law, this report helps lead to the allocation of much needed funding and resources to el and systems in the states and at the local level.

1 It is within the purview of the states to administer elections.[18] And although members of Congress may not have a direct hand in the processes and procedures for carrying out elections, they still have a role to play by ensuring elections are properly and adequately funded. Nearly three-quarters of states are estimated to have less than 10 percent of funding remaining from the Help America Vote Act, which allocated nearly $4 billion in 2002 to help states with elections.[19] According to a 2017 report, 21 states support receiving more funding from the federal government to help secure elections.[20]

2 All 50 states have taken at least some steps to provide security in their election administration. In recent examples:

- Virginia overhauled its paperless direct recording electronic voting machines and switched to a statewide paper ballot voting system just weeks before the 2017 elections.
- In 2017, Colorado became the first state to carry out mandatory risk-limiting post-election audits.
- In 2017, Rhode Island passed a bill requiring risk-limiting post-election audits for future elections.
- A new election vendor contract in Alabama requires election officials with access to the state's voter registration system to undergo cybersecurity training prior to elections.
- In December 2017, New York Gov. Andrew Cuomo (D) announced a new election security initiative as part of his 2018 State of the State agenda, including creating a state Election Support Center, developing an Elections Cyber Security Support Toolkit, and providing Cyber Risk Vulnerability Assessments and Support for Local Boards of Elections, among other things.
- At least 36 states are coordinating with or have already enlisted some help from DHS or the National Guard in assessing and identifying potential threats to voter registration systems.

voting systems with technology that produces voter verified paper ballots, and Indiana is considering implementing risk-limiting post-election audits for the 2018 elections. Florida Gov. Rick Scott (R) has requested millions of dollars in funding aimed at protecting election systems and software from attack. And on February 9, Gov. Tom Wolf's (D) administration in Pennsylvania—which still uses paperless voting machines in some jurisdictions—ordered counties looking to replace voting systems to purchase machines with paper records.

4 No state received a perfect score in this report. With few exceptions, most states fell in the middle of the spectrum: No state received an A; 11 states received a B; 23 states received a C; 12 states received a D; and five states received an F.

5 The main takeaway from the Center for American Progress' research and analysis is that all states have room for improvement:

- Fourteen states use paperless DRE machines in at least some jurisdictions. Five states rely exclusively on paperless DRE machines for voting.
- Thirty-three states have post-election audit procedures that are unsatisfactory from an election security standpoint, due either to the state's use of paperless DRE machines, which cannot be adequately audited, or other factors. At least 18 states do not legally require post-election audits or require jurisdictions to meet certain criteria before audits may be carried out.
- Thirty-two states allow regular absentee voters and/or U.S. citizens and service members living or stationed abroad to return voted ballots electronically, a practice deemed insecure by election and cybersecurity experts.
- At least 10 states do not provide cybersecurity training to election officials.

6 This point cannot be overemphasized: Even states that received a B or a C have significant vulnerabilities that leave them susceptible to hacking and infiltration by sophisticated nation-states. However, by making meaningful changes to how elections are carried out, states can improve their overall election security while supporting public confidence in election procedures and outcomes.

7 The election security factors considered in this report were selected based on their ability to evaluate election security and preparedness at the state level. They are:

1. Minimum cybersecurity standards for voter registration systems
2. Voter-verified paper audit trail
3. Post-election audits that test election results
4. Ballot accounting and reconciliation
5. Return of voted paper absentee ballots
6. Voting machine certification requirements
7. Pre-election logic and accuracy testing

8 The information included in this report is derived primarily from state statutes and regulations, as well as interviews with state and local election officials. A debt of gratitude is owed to several organizations for the work they've conducted on the seven categories considered in this report, including the Brennan Center for Justice, Common Cause, Verified Voting, the Pew Charitable Trusts, and the National Conference of State Legislatures. We also drew from information supplied by the U.S. Election Assistance Commission.

9 As part of our research, we reached out to the offices of the top election official in all 50 states plus the District of Columbia, requesting phone interviews to verify research and provide election officials the opportunity to expand on state requirements. In addition to requesting phone conversations, we sent state election offices a survey covering our areas of interest, which we invited them to complete in the event that they were unable to speak over the phone. The authors requested a follow up phone interview with any state that opted to fill out the survey. Finally, each state was given the opportunity to review and comment on our assessments prior to the publication of this report.

10 For grading each state's level of election security preparedness, we awarded points based on a state's adherence to a set of best practices included within each category. Each of the seven

could receive was 15 points. In four categories, if a state adheres to all the best practices included within a category it received a "fair" score, and 1 point for that category. If the state adheres to some standards, but not others, it received a score of 0, or "unsatisfactory."

11 Three key categories were graded on a 3-point scale, those being voter-verified paper audit trail, post-election audits, and minimum cybersecurity standards for voter registration systems. The 3-point scale was assigned to categories that, if implemented correctly, are found to greatly improve election security and where the standards were numerous, so it made sense to supplement the category with the opportunities to earn additional points.

12 The point distribution varies slightly for these three categories. For example, states that carry out elections through the exclusive use of paper ballots received 3 points, or a "good" score, for that category. States that use VVPR-producing DRE machines statewide or in combination with paper ballots and/or ballot marking devices received a "fair" score. While recognizing that paper ballots are the most hack-proof way of conducting elections, we still wanted to recognize states using DRE machines that provide a paper record of votes cast. If a state uses paperless DRE machines in any of its jurisdictions, it received an "unsatisfactory" score for that category.

13 For the category of post-election audits, this report identifies nine best practices for carrying out such audits. Because robust post-election audits are considered particularly important for improving election security, states must adhere to all nine of those best practices to receive a "good" score for this category. States that meet seven or eight standards received a "fair" score, and meeting three to six standards earned a state a "mixed" score. Failing to adhere to at least two "best practices" resulted in the state receiving 0 points for this category. Even if a state met a majority of the best practices included in this category, it could still receive an "unsatisfactory" score if it failed to meet the best practices of making audits mandatory or controlling for erroneous preliminary outcomes, as these are particularly important for carrying out meaningful post-election audits. A state also automatically earned an "unsatisfactory" score for this category if it uses paperless DRE machines in any jurisdictions, as these machines are impossible to adequately audit.

14 The category of minimum cybersecurity standards for voter registration systems is one of those where the recommended minimum standards are so numerous that it made sense to provide states with the opportunity to earn additional points for adhering to all or almost all of the recommendations. The scoring for this category differed slightly depending on whether the state

not to use electronic poll books, the two recommended standards relating to electronic poll books were not considered for scoring states that do not use them. Thus, states that use electronic poll books were measured against a total of eight standards, while states that do not use electronic poll books—or are only in the early piloting stages of using electronic poll books—were measured against a total of six standards, as detailed further below.

[5] Each individual best practice standard within a given category was given equal weight, aside from the exceptions mentioned above.

[6] In some cases, information on a state's adherence to cybersecurity standards for voter registration systems was difficult to find. There are many reasons states may have for keeping information on specific cybersecurity requirements of state-run databases private and inaccessible to the public, including researchers. Throughout our research, we made numerous attempts to reach out to state officials about their states' cybersecurity requirements and practices for voter registration. Unfortunately, some states failed to respond to our requests for information and comment, while others refused to do so, citing legal or security reasons in some cases. As a result, we were unable to award these states credit for certain cybersecurity standards due to missing pieces of information. This is not to say that these states do not in fact require these important security measures, but rather that we were unable to award credit to the state for information that was not provided. In such cases, states received an "incomplete" for the cybersecurity category with missing information, but were awarded credit where possible based on the information we did have. We felt that this was the fairest way to handle the point distribution, as we did not want to deter states from sharing information with us or punish those states that did share information on voter registration cybersecurity. To increase transparency and public confidence in U.S. elections, it is important that the public have access to information about the measures that states are taking to protect voter data. Notably, states with an "incomplete" score in the cybersecurity category may have a higher score overall if they are in fact carrying out the missing standards. However, at most, a state with an "incomplete" score in the cybersecurity category would raise its grade by only one letter grade if it adheres to all the missing best practices standards in that category. In most cases, a state's grade would not change at all given the point distribution for other categories. We indicate that a state's grade may be higher by way of a solidus or forward slash (Example: D/C) if there was information missing on a state's voter registration cybersecurity requirements and if the state's overall grade would change if it is carrying out the missing cybersecurity best practices.

certain data points may need updating as state laws and practices change or more information becomes available. Information contained in this report reflects research and analysis at the point of publication.

18 The grades for each state were assigned per the following point distribution:

- A = 13 points
- B = 10 points to 12 points
- C = 7 points to 9 points
- D = 4 points to 6 points
- F = 1 point to 3 points

19 A more comprehensive description of the standards and explanation of the best practices against which states were graded is below.

Category 1: Cybersecurity standards for voter registration systems

20 Some states still use voter registration databases that are more than a decade old, leaving them susceptible to modern-day cyberattacks.[21] If successfully breached, hackers could alter or delete voter registration information, which in turn could result in eligible voters being turned away at the polls or prevented from casting ballots that count. Hackers could, for example, switch just a few letters in a registered voter's name without detection.[22] In states with strict voter ID laws, eligible voters could be prevented from voting because of discrepancies between the name listed in an official poll book and the individual's ID. In addition, by changing or deleting a registered individual's political affiliation, hackers could prevent would-be voters from participating in partisan primaries.

21 There are serious privacy implications associated with breaches to voter registration databases. Voter registration lists contain myriad personal information about eligible voters—including names, addresses, dates of birth, driver's license numbers, political affiliations, and partial Social Security numbers—that could be used by foreign or domestic adversaries in any number of ways.[23] Moreover, while electronic poll books have been shown to increase efficiency and reduce wait

system. ... Guarding voter registration systems against hacking and manipulation is therefore critically important to protecting the right to vote and voter privacy.

12 It is worth noting that the recommendations listed below represent minimum cybersecurity standards that states should have in place to protect their voter registration systems. We sought to frame our inquiry into state voter registration systems broadly to avoid providing any kind of road map to potential malicious actors. We know that there are cybersecurity standards beyond those listed below that states should adopt in order to protect voter information, and we recommend that election officials work with cybersecurity experts in implementing them. For example, all states should have a backup voter registration database available in case emergencies arise.

13 The factors considered for grading in this category are:

- **Whether the state's voter registration system provides access control to ensure that only authorized personnel can access the voter registration database.** Access control is perhaps the most basic cybersecurity requirement that all states should implement to prevent unauthorized access to voter registration databases and sensitive voter information.[25] Access control measures can consist of anything from single or multifactor authentication to IP-recognition software, ensuring that only those with permission have access to the voter registration system.

- **Whether the state's voter registration system has logging capabilities to track modifications to the voter registration database.** Logging capabilities allow cyberprofessionals to monitor activity—innocent and malicious—on databases containing sensitive information.[26] When used, the software records all changes made to a database, oftentimes along with the name or IP address of the user responsible. A timestamp of when the change was made is also often provided.[27] Logging capabilities assist with investigations into suspicious cyberactivity by allowing cyberanalysts to identify and track those responsible.

- **Whether the state's voter registration system includes an intrusion detection system that monitors a network of systems for irregularities.** As the name suggests, intrusion detection systems monitor networks and computers for malicious or anomalous activity and alert relevant parties when potential problems arise.[28] Intrusion detection systems can include firewalls, anti-virus software, and spyware detection programs, to name just a few.[29] Given the increasing frequency and growing sophistication of modern-day cyberattacks, state officials

accordingly to prevent the loss or alteration of sensitive information.

- **Whether the state performs regular vulnerability analysis on its voter registration system.** To understand the full extent of election-related risk, vulnerability assessments should be carried out continuously on voter registration databases. By conducting regular vulnerability assessments, the state can identify the existence and extent of potential weakness within its voter registration system. By doing so, election officials can better determine where government resources should be allocated and plan for preventative measures and strategies.

- **Whether the state has enlisted DHS or the National Guard to help identify and assess potential threats to its voter registration system.** While it is important for states to retain a level of autonomy over the administration of their elections, many states lack the personnel and resources necessary to thoroughly probe and analyze complex cybervulnerabilities in election databases and machines. Federal agencies and military personnel with expertise in cybersecurity and who may be privy to classified information on contemporaneous cyberthreats should be responsible for carrying out comprehensive threat assessments on election infrastructure.[30] By combining their expertise on cyberthreats and insight into the unique qualities of localized election infrastructure, state and federal officials can better assess and deter attempts at electoral disruption.[31] DHS services—which can include cyberhygiene scans, risk and vulnerability assessments, and incident response assistant, among other things[32]—come at no cost to the states.[33]

- **Whether the state provides cybersecurity training to election officials.** Election officials are on the front lines of guarding U.S. elections against attack by foreign and domestic actors, as well as a host of other potential Election Day problems. However, few election officials possess the kind of cybersecurity expertise necessary to detect and protect against potential attacks.[34] Even basic training to identify spear-phishing attempts and respond to other suspicious cybernetwork activity can go a long way toward improving election security.

14 For states that use electronic poll books, additional considerations are:

- **Whether the state requires that all electronic poll books undergo testing before Election Day.** As with all voting machines, electronic poll books should be tested prior to Election Day to ensure that they are in good and proper working order. In doing so, election officials can avoid machine malfunctions on Election Day that result in long lines for voters, which can hinder

- **Whether backup paper voter registration lists are available at polling places using electronic poll books on Election Day.** To ensure that voter registration lists are accessible during voting periods, states should establish paper-based contingency plans during early voting and on Election Day in case electronic poll books experience malfunctions or hacking. Each polling place that uses electronic poll books should be required to have paper copies of its voter registration lists available that can be consulted throughout the voting process in case of emergency.

Points were distributed for this category as follows, depending on whether the state uses electronic poll books:

States using electronic poll books:

State adheres to eight best practices: Good, 3 points

State adheres to six or seven best practices: Fair, 2 points

State adheres to three to five best practices: Mixed, 1 point

State adheres to zero to two best practices: Unsatisfactory, 0 points

States not using electronic poll books:

State adheres to six best practices: Good, 3 points

State adheres to four or five best practices: Fair, 2 points

State adheres to two or three best practices: Mixed, 1 point

State adheres to zero or one best practices: Unsatisfactory, 0 points

We also provide information on the estimated age of a state's voter registration system. This information was not factored into the point distribution. However, we felt it was important to include in order to provide a fuller picture of voter registration system cybersecurity.

that a state can take to improve election security is updating its voter registration system to support software upgrades that guard against and prevent modern-day cyberattacks. Research has been done on the threat posed by outdated voting registration systems.[36] Outdated voter registration systems often lack the specific hardware and software components necessary to adequately guard against modern-day cyberthreats, leaving states vulnerable to hacking and system crashes.[37] Some state voter registration systems, for example, still run on outdated and unsupported software such as Windows XP or Windows 2000.[38] However, even an updated voter registration system can be vulnerable to attack if the state fails to put into place other basic cybersecurity standards that monitor and protect the system.

Category 2: Voter-verified paper audit trail

7 Confirmation that votes were correctly counted cannot be provided unless a reliable auditable paper trail exists that can be checked against the official election outcome. Paper ballots that are tabulated by optical scanning machines and voter-verified paper records produced by DRE machines offer a record of voter intent, which will exist even if voting machines are attacked and data are altered. Admittedly, paper ballots and records can only help detect malicious activity after votes are cast, and only if robust post-election audits are conducted with the ability to detect and remedy erroneous preliminary outcomes. However, conducting elections with paper-based voting systems is one of the most important steps states can take to improve election security. They are necessary both to conduct meaningful post-election audits that can confirm the election outcomes and to enable post hoc correction in the event of malfunction or security breaches.

8 Given the importance of having a voter-verified paper audit trail, states received "good" scores—a full 3 points—if they carry out elections using paper ballots statewide. Because evidence has shown that all electronic voting machines are vulnerable to manipulation, voting on paper is the most hack-proof way of conducting elections. Of course, even electronic tabulating equipment such as optical scan machines can be hacked. However, at least with a paper ballot, election officials have a hard copy to go back to in order to verify the voter's selection. As such, paper ballots are preferable from an election security standpoint even to DRE machines with VVPR, which allow voters to review the machine's reading of their vote prior to casting, although it is uncertain that all voters do so.

9 However, because DRE machines with VVPR leave a paper record that can be used in post-election audits, we awarded states that use such machines exclusively or in combination with paper ballots

combination with paper ballots and/or ballot marking devices received a "satisfactory" score. If a state uses paperless DRE machines in any of its jurisdictions, it automatically received an "unsatisfactory" score for this category.

10 Federal law requires all states to have a minimum number of electronic voting machines available for accessibility purposes. Because those machines are necessary in order to accommodate and facilitate voting among people with disabilities and comply with requirements set out in the Help America Vote Act of 2002, their use in states for this limited purpose was not considered for grading purposes.

11 Points were distributed for this category as follows:

12 State only uses paper ballots statewide: Good, 3 points

13 State uses VVPR-producing DRE machines statewide or in combination with paper ballots and/or ballot marking devices: Fair, 2 points

14 State uses paperless DRE machines in any of its jurisdictions: Unsatisfactory, 0 points

15 **States that allow voting by mail were awarded a full 3 points for this category given that the overwhelming majority of voters in those states use paper ballots. This is true even though most vote-by-mail states make some DRE machines with VVPR available at vote centers, though mostly for accessibility purposes.*

Category 3: Post-election audits

16 Because all voting machines are vulnerable to hacking, misprogramming, and even to using the wrong kind of pen to mark ballots, it is of the utmost importance that election officials conduct robust post-election audits that have a large chance of catching and correcting wrong outcomes. Even jurisdictions that hand-count all ballots should carry out post-election audits, as the counting process can be mired in human error. Importantly, an audit is only as good as the reliability of the ballots it tests. Therefore, meaningful post-election audits can only be conducted in states with strong voter-verified paper audit trails.

machines to ensure they have been properly aggregated on a fixed-percentage or fixed-number of audit units. Risk-limiting audits—considered the "gold standard" of post-election audits—increase the efficiency of the auditing process by testing only the number of ballots needed to determine the accuracy of election outcomes. Risk-limiting audits include an initial sample of ballots, based on the margin of victory, which are interpreted by hand. Depending on the results of the initial manual count, the audit may expand. As a result, risk-limiting audits offer election administrators an effective and efficient way to test the accuracy of an election without breaking the bank. Risk-limiting audits are the only kind of audit that can determine with a high degree of confidence that election outcomes are correct and have not been manipulated. However, as risk-limiting audits are a relatively new proposal and are just being adopted by states, we graded states for the existence of the audit practices they do have that function to confirm that ballots have been counted as cast.

18 The factors considered for grading in this category include:

- **Whether post-election audits are mandatory.** Post-election audits must be carried out after every election to confirm the accuracy of election outcomes. By only conducting audits after certain elections, states leave themselves vulnerable to hackers who can target unaudited races and election years. Moreover, tabulating machines can malfunction at any time and during any election. Audits must be carried out any time election results matter, meaning after every single election.
- **Whether the audit is conducted by a manual hand count.** Some states use the term "audit" to describe the process of simply rescanning batches of ballots after an election. Relying on these electronic scans—which are as vulnerable as any other computer data—limits the kinds of problems these reviews can detect. The scans aren't like photographs; they can differ due to machine error, tampering, or human error.[39] To trust that audit results are correct, auditing procedures must be software-independent. As long as an audit depends on electronic tabulators or devices, it can be hacked or manipulated. We recognize that manual audits can require resources—funding and personnel—that some localities may lack. However, in this day and age, where cyberintrusions by nation-states are an ever-growing threat, post-election audits—which are vitally important to election security—must be carried out by hand. The threat is simply too great to leave audits in the control of hackable machines and devices.

significant number tied to the specific margin of victory in one of more ballot contests. Tying the number of ballots included in a post-election audit to the margin of victory in one of more ballot contests—rather than a fixed-percentage or number—ensures that enough ballots are examined to create convincing evidence that the outcome is correct, and it also saves resources. For example, if the margin of victory between the winner and loser of a ballot contest is quite large, there is a high likelihood that the auditing of even a small batch of ballots will confirm the accuracy of the election outcome, which saves election officials time and resources. Alternatively, if the margin of victory is small, more ballots need to be audited because there is less room for error. While a more expansive audit requires expending more time and resources on the auditing process, doing so results in greater certainty that the election outcome is correct.

- **Whether the ballots, machines, or jurisdictions selected for the audit are chosen at random.** Random selection of the election components included in a post-election audit is necessary in order to prevent hackers from putting in place plans and procedures to rig the post-election audit process or from targeting specific machines or ballot categories that they know will not be included in the audit.

- **Whether all categories of ballots—regular, early voting, absentee, provisional, and UOCAVA—are eligible for auditing.** All ballot types should be eligible for inclusion in post-election audits. By only auditing certain categories of ballots, election officials may fail to detect anomalies in the tabulation of other ballot types. This is particularly important in states where absentee, early voting, or provisional voting is popular among voters. For example, in North Carolina, at least 56,000 provisional and absentee ballots were cast during the 2016 election.[40] By failing to include all ballot types in the auditing process, states can exclude from testing and analysis ballots that have the potential to alter election outcomes.

- **Whether the audit can escalates to include more ballots.** If an audit fails to find strong enough evidence that the preliminary outcome is right, it should escalate to include more ballots to ensure confidence in election results. Escalation should lead to a full recount if necessary.

- **Whether the audits are conducted in a public forum or the results made immediately available for public review.** Post-election audits should either be open to public observance or the results made publicly available in order to increase transparency and public confidence in the accuracy of election outcomes.

Results: Post-election audits should be carried out after preliminary outcomes are announced, but before official certification of election results. This gives election officials enough time for escalation and correction of preliminary results if preliminary election outcomes are found to be incorrect. That said, post-election audits conducted after certification can still be useful if they have the ability to overturn the certified results if the audit finds they are wrong.

- **Whether the audit can correct the preliminary result of an audited contest if it discovers that the preliminary result was wrong.** In other words, do audits control the overall results? To be meaningful, post-election audit results must be able to reverse preliminary outcomes if the audit determines they are incorrect. The utility of post-election audits depends on their ability to correct incorrect election results.

Points were distributed for this category as follows:

State adheres to nine best practices: Good, 3 points

State adheres to seven or eight best practices: Fair, 2 points

State adheres to three to six best practices: Mixed, 1 point

State adheres to zero to two best practices: Unsatisfactory, 0 points

**A state received an "unsatisfactory" score for this category if (1) the state's post-election audits are not mandatory, (2) the results are not binding on official election outcomes, or (3) the state uses paperless DRE machines—which are not auditable—in any jurisdiction. This was true even if the state adheres to a majority of the other best practices included within this category. The added weight does not work in reverse. For example, if a state met only six of the standards—including that the audit is mandatory and binding—its score would not be raised from "mixed" to "fair."*

Category 4: Ballot accounting and reconciliation

A paper-based voting system must be combined with strong ballot accounting and reconciliation requirements and procedures. Ensuring that all ballots—used and unused—are accounted for at the close of Election Day and that all votes are included in the final vote tally is one of the most basic and important ways that election officials can improve the security of their elections. By doing

invalid ballots being added, causing incorrect vote counts. A great deal of the research on state ballot accounting and reconciliation included in this section is derived from a comprehensive 2012 report from Common Cause, Verified Voting, and Rutgers School of Law entitled "Counting Votes 2012: A State by State Look at Voting Technology Preparedness."[41] While we relied on the research by the authors of that report, we conducted a thorough review to update the research where there had been changes in the law.

The factors considered for grading in this category include:

- **Whether all ballots are accounted for at the precinct level.** Before vote totals can be accumulated by the state, local election officials must tally and account for all ballots—used and unused—at individual polling places or at vote centers. Precinct officials are best positioned to account for the ballots they received and ballots that have been cast, spoiled, or unused, or that were submitted provisionally. As such, this process should be completed at the local level.
- **Whether precincts are required to compare and reconcile the number of ballots cast with the number of voters who signed in at the polling place.** Part of the ballot accounting and reconciliation process involves comparing the number of ballots to the number of voters who showed up to the polls to participate in the electoral process. Only through comparing the number of votes to the number of voters can election officials be confident that ballots have not been removed or brought into the polling place from elsewhere. In reconciling these numbers, poll workers should be prohibited from randomly discarding any excess ballots. As the authors of "Counting Votes 2012" found, and as our independent review confirmed, some states still allow this ill-advised practice and lost a point for this category as a result.[42]
- **Whether county officials are required to compare and reconcile precinct totals with countywide results to ensure that they add up to the correct number.** Once they receive and conglomerate vote totals, county officials should examine and compare the countywide results to tallies submitted by the precincts to make sure that they add up to the correct number. Doing so provides election officials with some assurance that the results are correct and can help to detect a computing error if one exists.

Points were distributed for this category as follows:

State adheres to zero to two best practices: Unsatisfactory, 0 points

We provide additional information on state ballot accounting and reconciliation procedures that was not factored into the point distribution as wide variation and lack of visibility make them difficult to evaluate; however, we felt it was important to include the information in order to provide a fuller picture of state practices in this area.

- **Whether counties are required to review and account for all voting machine memory cards and flash drives to ensure that they have been properly loaded onto the tally server.** Our democracy depends on every valid vote being counted on Election Day. As such, it is critically important that election officials review status reports from electronic tally servers in states that use them in order to ensure that all voting machine memory cards and flash drives are properly uploaded and counted. In some states, the electronic management software that tabulates results provides a warning if all memory cards or flash drives that were created for an election are not properly uploaded. Electronic systems are more convenient, but they are prone to hacking or manipulation by sophisticated actors. As such, any review process should ideally be software-independent.
- **Whether the state requires that vote tallies and any ballot reconciliation information be made public.** Transparency is necessary for all election processes—especially those involving vote totals—in order to establish public confidence in the electoral system and election outcomes. By making information available on election results for each candidate and ballot issue, as well as the ballot reconciliation processes that were used to reach those results, states can improve public confidence in their elections.

Category 5: Return of voted paper absentee ballots

Electronic absentee voting—or the return of voted absentee ballots electronically via email, fax, or web portal—is risky because there is no way for absentee voters to know whether the votes they cast are being accurately recorded. While 29 states only allow electronic submission for UOCAVA voters, three states allow any absentee voter to return completed ballots electronically.[43]

Most experts agree that returning voted ballots electronically is not safe. An official from DHS's Cyber Security Division warned that "online voting, especially online voting in large scale,

accounting and security of their votes and provides an avenue for malicious actors to manipulate the voting results."[44] The National Institute of Standards and Technology has also warned against online voting.[45] Furthermore, it is impossible to carry out meaningful post-election audits on voted ballots submitted electronically because there is no reliable paper record that can be referenced during the auditing process.

[3] Of course, it is of utmost importance that military personnel and U.S. citizens stationed and living overseas are provided opportunities to vote and have their voices heard in our democracy. It is equally important, however, that their votes be delivered securely and their privacy protected. Currently, that means returning a hard copy paper ballot via U.S. mail. Requiring UOCAVA voters to return ballots by mail does not appear to have a significant impact on ballot return rates. If we base projections of UOCAVA ballot return rates on information contained in Pew surveys of unreturned UOCAVA ballots in the states in 2012 and 2014,[46] we see that see that states requiring UOCAVA voters to return voted ballots via mail actually had a slightly higher return rate those years than states that permit voted ballots to be returned electronically.[47]

[4] For this category, states were graded simply on whether they require voted absentee ballots to be returned by mail (or in person). If so, a state received a "fair" score—or 1 point—for that category. If the state allows any voters, including regular absentee or UOCAVA voters, to return ballots electronically—via email, fax, or web portal—it received an "unsatisfactory" score, or 0 points.

[5] Some feel that the return of voted ballots electronically constitutes a significant threat to election security, on par with use of paperless DRE machines, lack of minimum cybersecurity standards for voter registration systems, and inadequate auditing procedures.[48] Of course, that number assumes that all UOCAVA voters in those states would return their ballots via internet, which is not likely the case. Some may opt to return their voted ballots by mail. Moreover, the EAC has not yet come out with their 2016 numbers and UOCAVA reliance on internet voting may have changed since 2012. However, the EAC data offers a rough estimate of how many ballots could be at risk in future elections. U.S. Election Assistance Commission, "Uniformed and Overseas Citizens Absentee Voting Act" (Washington: EAC, 2013), available at https://www.eac.gov/assets/1/28/508compliant_Main_91_p.pdf.] While we share concerns over electronic absentee voting, we reserved the weighted point distribution for those three categories listed above.

16 This category is concerned more with preventing machine malfunction than hacking. Even new machines that are certified and tested to federal requirements are vulnerable to hacking and manipulation by sophisticated actors. Even so, for the purposes of preventing Election Day disruptions, the basic technological requirements that voting machines must adhere to before being purchased and used in a state are worth consideration.[49]

17 States should ensure that any machine they purchase adheres to the Election Assistance Commission's Voluntary Voting System Guidelines. The EAC's guidelines require voting machines and components to meet minimum security, functionality, and accessibility standards. Some states have their own certification requirements that either substitute or supplement the EAC's voluntary guidelines, and indeed some experts feel the federal certification process as a whole needs updating. However, we feel that adherence to a uniform set of standards helps to ensure basic functioning and efficiency for voting machinery and equipment. The EAC anticipates finalizing a new set of voting system guidelines in 2018, which will take into account advances in technology and emphasizes auditable voting systems and evidence-based elections.[50] Leaving the standard-setting process to the states can be an overwhelming task for state officials and can result in a mishmash of voting machine requirements across the country with varying degrees of thoroughness and stringency. Indeed, in speaking about federal voting machine standards, Rhode Island Secretary of State Nellie Gorbea said, "We in Rhode Island could not come up with as good and as fast a process for what the EAC already had with regards to general voting equipment guidelines."[51] As an alternative to requiring that all voting machines be EAC-certified, states may require that voting machines undergo review by a federally accredited laboratory or have statutory requirements that all voting machines must meet or exceed the federal standards.

18 Abiding by the EAC's Voluntary Voting System Guidelines is not foolproof against hacking or malfunction. Even EAC-certified voting machines can be hacked or experience problems. Therefore, it is again important to emphasize the importance of paper-based voting systems with voter-verified paper audit trails, which can be referred to if complications arise.

19 For this category, a state was graded on whether it requires its voting machines to be EAC certified, adhere to federal standards, or undergo testing by an EAC accredited laboratory. If so, a state received a "fair" score—or 1 point—for this category. If not, a state received an "unsatisfactory" score—or 0 points—for this category.

that are at least a decade old.[52] Old voting machines pose serious security risks and are susceptible to system crashes, "vote flipping," and hacking, as many rely on outdated computer operating systems that do not accommodate modern-day cybersecurity protections.[53] Moreover, upkeep for outdated machines is becoming increasingly difficult, because many parts are no longer manufactured. According to experts, the predicted lifespan for most voting machine models is around 10 years.[54] Adding to this, experiments conducted by computer scientists on electronic voting machines have shown that they are easily hacked, can be reprogrammed to predetermine electoral outcomes, and are susceptible to malicious vote-stealing software.[55] While more long-term solutions to fixing flaws in voting machine architecture may be required,[56] one thing states can do right now to better protect against machine malfunction and Election Day disruptions is to invest in replacing all outdated voting machines. This would include switching to a paper ballot system with new optical scan machines.

11 As stated previously, just because a voting machine is new does not mean that it is safe from hacking and malfunction. While newer machines may include updated software components that lend some protection against system failure, all electronic voting machines are potentially vulnerable to problems and disruption. It is for this reason that any new voting machine must be accompanied by a paper ballot component or voter-verified paper trail that can be referred to in case problems arise.

12 We recognize that in many states new voting machines are purchased by the counties rather than at the state level. Even when this is the case, however, states and the federal government should assist localities in purchasing new machines by providing adequate funding.

Category 7: Pre-election logic and accuracy testing

13 As with the previous section, this category is concerned more with preventing machine malfunction than hacking. Logic and accuracy testing is not foolproof. Indeed, sophisticated hackers can manipulate pre-election testing procedures by installing malware that remains inactive during pre-election tests but activates during voting periods. Even so, pre-election testing remains a basic step that election officials can take to help detect possible machine errors and address machine-related problems prior to Election Day.

whether the machines that will be used on Election Day or during early voting will function correctly when voters show up to vote. Pre-election logic and accuracy testing should be mandatory and should be conducted on all machines that will be used for voting or to tabulate ballots during an election. Most states already have laws in place requiring state officials to test voting machines and equipment in the weeks and months leading up to an election, although their scope varies depending on the jurisdiction.[57] Some states require that all voting machines be tested, while others limit testing to only a small sample.

It is important that all voting machines that will be used in an upcoming election be tested prior to Election Day to ensure that they will accurately read and tabulate votes during voting periods. By testing only a small number or percentage of machines, states may allow other machines with potential problems to slip through the cracks.

For this category, states were graded on whether election officials are required to perform pre-election logic and accuracy testing on all voting machines that will be used in an election. If so, the state received a "fair" score—or 1 point—for this category. If not, the state received an "unsatisfactory" score—or 0 points—for this category.

We also provide information on some specific pre-election logic and accuracy testing procedures. This information was not factored into the point distribution; however, we felt it was important to include it in order to provide a fuller picture of state practices related to pre-election machine testing.

- **Whether the testing is open to the public.**[58] Pre-election logic and accuracy testing should take place in a public forum with appropriate public notice, thereby increasing transparency and public confidence in the election process.
- **Whether testing is conducted close to the election, but with enough time to allow for effective remediation.** Testing should be carried out close enough to an election to ensure that the machines are in a similar condition to Election Day as they were at the time of testing, but with enough time for election officials to reprogram or replace voting machines that exhibit problems during testing.

- Massachusetts
- Michigan
- Minnesota
- Mississippi
- Missouri
- Montana
- Nebraska
- Nevada
- New Hampshire
- New Jersey
- New Mexico
- New York
- North Carolina
- North Dakota
- Ohio
- Oklahoma
- Oregon
- Pennsylvania
- Rhode Island
- South Carolina
- South Dakota
- Tennessee

- Utah
- Vermont
- Virginia
- Washington
- West Virginia
- Wisconsin
- Wyoming

About the authors

Danielle Root is the voting rights manager for Democracy and Government at the Center for American Progress.

Liz Kennedy is the senior director of Democracy and Government Reform at the Center.

Michael Sozan is a senior fellow at the Center, where he focuses on democracy and government reform.

Jerry Parshall is a manager of State and Local Government Affairs at the Center.

Endnotes

1. Associated Press, "Federal Government Tells 21 States Election Systems Targeted by Hackers," September 22, 2017, available at https://www.nbcnews.com/storyline/hacking-of-america/federal-government-tells-21-states-election-systems-targeted-hackers-n804031.
2. Callum Borchers, "What we know about the 21 states targeted by Russian hackers," *The Washington Post*, September 23, 2017, available at https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/?

3. Scott Bauer, "Homeland Security now says Wisconsin elections not targeted," Associated Press, September 27, 2017, available at https://www.apnews.com/10a0080e8fcb4908ae4a852e8c03194d; David Shepardson, "California, Wisconsin deny election systems targeted by Russian hackers," Reuters, September 28, 2017, available at http://www.reuters.com/article/us-usa-election/california-wisconsin-deny-election-systems-targeted-by-russian-hackers-idUSKCN1C32SQ?utm_source=applenews; ABC News, "Texas says DHS Wrong, hacker didn't target state," September 28, 2017, available at http://abcnews.go.com/amp/Technology/wireStory/latest-texas-dhs-wrong-hacker-target-state-50168406; Cynthia McFadden and others, "Russians penetrated U.S. voter systems, top U.S. official says," NBC, February 8, 2018, available at https://www.nbcnews.com/politics/elections/russians-penetrated-u-s-voter-systems-says-top-u-s-n845721.

4. Justin Volz and Jim Finkle, "Voter Registration Databases in Arizona and Illinois Were Breached, FBI Says," Time, August 26, 2016, available at http://time.com/4471042/fbi-voter-database-breach-arizona-illinois/; Associated Press, "Federal Government Tells 21 States Election Systems Targeted by Hackers"; Callum Borchers, "What we know about the 21 states targeted by Russian hackers."

5. Associated Press, "Federal Government Tells 21 States Election Systems Targeted by Hackers."

6. Peter Baker and David E. Sanger, "Trump-Comey Feud Eclipses a Warning on Russia: 'They Will Be Back,'" *The New York Times*, June 10, 2017, available at https://www.nytimes.com/2017/06/10/us/politics/trump-comey-russia-fbi.html.

7. Joe Uchill, "Hackers breach dozens of voting machines brought to conference," *The Hill*, July 29, 2017, available at http://thehill.com/policy/cybersecurity/344488-hackers-break-into-voting-machines-in-minutes-at-hacking-competition.

8. Peter Reuell, "Voting-roll vulnerability," *Harvard Gazette*, September 6, 2017, available at https://news.harvard.edu/gazette/story/2017/09/study-points-to-potential-vulnerability-in-online-voter-registration-systems/.

9. Massimo Calabresi, "Inside Russia's Social Media War on America," *Time*, May 18, 2017, available at http://time.com/4783932/inside-russia-social-media-war-america/.

The Washington Post, January 4, 2016, available athttps://www.washingtonpost.com/local/virginia-politics/republican-yancey-picked-in-random-lottery-declared-winner-of-pivotal-va-house-race/2018/01/04/9c9caa5a-f0a1-11e7-b390-a36dc3fa2842_story.html?utm_term=.f49a8842bcae.

11. Associated Press, "Court rules Virginia House of Delegates race a tie," December 20, 2017, available at https://www.washingtonpost.com/lifestyle/kidspost/virginia-democrat-wins-house-of-delegates-seat-by-one-vote-according-to-recount/2017/12/20/eb856c20-e5ab-11e7-ab50-621fe0588340_story.html?utm_term=.8094d78d6da7.

12. *The New York Times*, "Full Transcript and Video: James Comey's Testimony on Capitol Hill," June 8, 2017, available at https://www.nytimes.com/2017/06/08/us/politics/senate-hearing-transcript.html.

13. During an interview with PBS News House, Sens. Amy Klobuchar (D-MN) and James Lankford (R-OK) expressed concern over the state election preparedness and timing of the 2018 elections but noted the potential for widespread vulnerability screenings for election systems and valuable information sharing between states and the federal government. PBS News Hour, "'42 states haven't upgraded their election equipment in over a decade and Russia knows it,'" January 10, 2018, available at https://www.pbs.org/newshour/show/42-states-havent-upgraded-their-election-equipment-in-over-a-decade-and-russia-knows-it; Martin Matishak, "The time to hack-proof the 2018 election is expiring — and Congress is way behind," *Politico*, November 26, 2017, available at https://www.politico.com/story/2017/11/26/election-cybersecurity-hackers-midterms-259472.

14. *The New York Times*, "Full Transcript and Video: James Comey's Testimony on Capitol Hill."

15. Danielle Root and Liz Kennedy, "9 Solutions to Secure America's Elections" (Washington: Center for American Progress, 2017), available at https://www.americanprogress.org/issues/democracy/reports/2017/08/16/437390/9-solutions-secure-americas-elections/.

16. Open Source Election Technology Institute, "Critical Democracy Infrastructure: Protecting American Elections in the Digital Age," September 2017, available at https://trustthevote.org/wp-content/uploads/2017/09/2017_oset-cdi_briefing1.pdf.

written on extensively in recent months and does not need repeating here. Latanya Sweeney, J. Su Yoo, and Jinyan Zang, "Voter Identity Theft: Submitting Changes to Voter Registrations Online to Disrupt Elections," Technology Science, September 06, 2017, available at https://techscience.org/a/2017090601.

18. U.S. Const. art. I, sec. 4, cl. 1, available at http://press-pubs.uchicago.edu/founders/tocs/a1_4_1.html.

19. Cory Bennett and others, "Cash-strapped states brace for Russian hacking fight," Politico, September 3, 2017, available at https://www.politico.com/story/2017/09/03/election-hackers-russia-cyberattack-voting-242266.

20. "Five are open to it if the money comes with no strings attached, three oppose it, and two say Congress should supply the remaining $395 million it has yet to provide from a pot of money it authorized in 2002." Bennett and others, "Cash-strapped states brace for Russian hacking fight."

21. Lawrence Norden and Ian Vandewalker, "Securing Elections From Foreign Interference" (Washington: Brennan Center for Justice, 2017), available at https://www.brennancenter.org/publication/securing-elections-foreign-interference.

22. A Republican data firm and GOP contractors reportedly leaked personal information belonging to nearly 200 million people in June 2017. See Selena Larson, "Data of Almost 200 Million Voters Leaked Online by GOP Analytics Firm," CNN, June 19, 2017, available at http://money.cnn.com/2017/06/19/technology/voter-data-leaked-online-gop/index.html; Wesley Bruer and Evan Perez, "Officials: Hackers Breach Election Systems in Illinois, Arizona," CNN, August 30, 2016, available at http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/index.html.

23. Transcript of "Senate Select Intelligence Committee Holds Hearing on Russian Interference in the 2016 Elections, Panel 2."

24. A used election poll book sold on eBay, for example, was recently found to still contain the personal information of 650,000 Tennessee voters after election officials failed to erase sensitive voter data. See Kevin Collier, "Personal Info of 650,000 Voters Discovered on Poll Machine Sold on Ebay," Gizmodo, August 1, 2017, available at http://gizmodo.com/personal-info-of-650-000-voters-discovered-on-poll-mach-1797438462; Lee and Liebling, "How Electronic

25. U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data," available at https://www.eac.gov/assets/1/28/Checklist_Securing_VR_Data_FINAL_5.19.16.pdf (last accessed September 2017).

26. U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

27. U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

28. U.S. Election Assistance Commission, "Checklist for Securing Voter Registration Data."

29. Margaret Rouse, "HIDS/NIDS (Host Intrusion Detection Systems and Network Intrusion Detection Systems)," available at http://searchsecurity.techtarget.com/definition/HIDS-NIDS (last accessed September 2017).

30. Researchers at RAND Corporation have estimated that there are more than 100,000 reservists with "some degree of cyber competence, including thousands with deep or mid-level cyber expertise." Researchers see the National Guard as an untapped cyber resource that has the potential to attract the very best in cyber industry and offer a valuable resource to states in protecting critical infrastructure. Isaac Porche and Brian Wisniewski, "Reservists and the National Guard offer uptapped resources for cybersecurity," Tech Crunch, April 18, 2017, available at https://techcrunch.com/2017/04/18/reservists-and-the-national-guard-offer-untapped-resources-for-cybersecurity/.

31. Isaac Porche, "Reservists and the National Guard offer untapped resources for cybersecurity," Tech Crunch, April 18, 2017, available at https://techcrunch.com/2017/04/18/reservists-and-the-national-guard-offer-untapped-resources-for-cybersecurity/.

32. Department of Homeland Security, "Statement by Secretary Johnson Concerning the Cybersecurity of the Nation's Election Systems," Press release, September 16, 2016, available at https://www.dhs.gov/news/2016/09/16/statement-secretary-johnson-concerning-cybersecurity-nation%E2%80%99s-election-systems.

33. There is a reported nine-month waiting list for some DHS state services related to election security. However, the National Defense Authorization Act (NDAA) for Fiscal Year 2018 authorizes the federal government to carry out a "Cyber Guard Exercise" on state election systems upon approval by the state. H.R.2810, available at https://www.congress.gov/bill/115th-congress/house-bill/2810/text?

Observe Cyber Guard Exercise," July 5, 2017, available at https://www.defense.gov/News/Article/Article/1238082/allies-partners-observe-cyber-guard-exercise/; Morgan Chalfant, "33 states accepted DHS aid to secure elections," The Hill, August 2, 2017, available at http://thehill.com/policy/cybersecurity/344981-33-states-accepted-dhs-aid-to-secure-elections.

34. Likhitha Butchireddygari, "Many County Election Officials Still Lack Cybersecurity Training," NBC News, August 23, 2017, available at https://www.nbcnews.com/politics/national-security/voting-prep-n790256.

35. Additional, nongraded information is indicated by gray font throughout the report.

36. Norden and Vandewalker, "Securing Elections From Foreign Interference."

37. Norden and Vandewalker, "Securing Elections From Foreign Interference."

38. Lawrence Norden, "We Need Election Integrity—Just Not the Way Trump Is Going About It," *Slate*, July 7, 2017, available at http://www.slate.com/articles/technology/future_tense/2017/07/the_real_way_to_fix_the_actual_election_tampering_crisis_in_the_u_s.html; Brian Barrett, "If You Still Use Windows XP, Prepare for the Worst," Wired, May 14, 2017, available at https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst/.

39. Philip B. Stark and Poorvi L. Vora, "Maryland Voting Audit Falls Short," *The Baltimore Sun*, October 28, 2016, available at http://www.baltimoresun.com/news/opinion/oped/bs-ed-voting-audit-20161028-story.html.

40. UCRJames, "How Many Absentee and Provisional Ballots are Left in FL and PA?," Daily Kos, November 14, 2016, available at https://www.dailykos.com/stories/2016/11/14/1599238/-How-Many-Absentee-and-Provisional-Ballots-are-Left-in-FL-and-PA.

41. Pamela Smith and others, "Counting Votes 2012: A State by State Look at Voting Technology Preparedness" (Washington and New Brunswick: Verified Voting, Common Cause, and Rutgers School of Law, 2012), available at http://countingvotes.org/sites/default/files/CountingVotes2012_Final_August2012.pdf.

42. Smith and others, "Counting Votes 2012."

The Washington Post, May 17, 2016, available at https://www.washingtonpost.com/news/post-nation/wp/2016/05/17/more-than-30-states-offer-online-voting-but-experts-warn-it-isnt-secure; National Conference of State Legislatures, "Electronic Transmission of Ballots," January 16, 2017, available at http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx.

44. Horwitz, "More Than 30 States Offer Online Voting, But Experts Warn It Isn't Secure."

45. National Institute of Standards and Technology, "NIST Activities on UOCAVA Voting," available at https://www.nist.gov/itl/voting/nist-activities-uocava-voting (last accessed September 2017).

46. In 2012, states with only mail-in returns had an average of 75 percent ballots returned while states with the electronic option had 73 percent of ballots returned. In 2014, states with only mail-in returns had an average of 62% ballots returned while states with the electronic option had 54 percent of ballots returned. The Pew Charitable Trusts, "Elections Performance Index," August 9, 2016, available at http://www.pewtrusts.org/en/multimedia/data-visualizations/2014/elections-performance-index#state-CT.

47. Ibid.

48. Indeed, If we base projections on EAC data for the 2012 general election, which examined the total number of UOCAVA ballots returned and submitted for counting that year (578,706), and compared that to the list of states that allow internet voting, we could expect more than 240,000 (243,5331 to be exact) UOCAVA ballots to be returned via internet in the 2020 election. [1

49. We did not consider whether a state's voting machines are connected to the internet. Today, most voting machines are not directly connected to the internet. It is important to note that machines can be hacked even if they aren't connected to the internet. Pam Fessler, "If Voting Machines Were Hacked, Would Anyone Know?", NPR, June 14, 2017, available at http://www.npr.org/2017/06/14/532824432/if-voting-machines-were-hacked-would-anyone-know; Jessica Schulberg, "Good News for Russia: 15 States Use Easily Hackable Voting Machines," The Huffington Post, July 17, 2017, available at https://www.huffingtonpost.com/entry/electronic-voting-machines-hack-russia_us_5967e1c2e4b03389bb162c96.

U.S. Election Assistance Commission, "Committee Approves Next Generation of Voting System Guidelines," Press release, September 12, 2017, available at https://www.eac.gov/news/2017/09/12/committee-approves-next-generation-of-voting-system-guidelines/; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines"; U.S. Election Assistance Commission, "Voluntary Voting System Guidelines 2.0," available at https://www.eac.gov/assets/1/6/TGDC_Recommended_VVSG2.0_P_Gs.pdf (last accessed January 2018).

51. Ben Berliner, "Some States Look to Feds for Help Replacing Old Voting Equipment," FCW, October 26, 2017, available at https://fcw.com/articles/2017/10/26/aging-voting-machines-berliner.aspx.

52. Additional, non-graded information is indicated by gray font throughout the report.

53. Brennan Center for Justice, "Voting System Security and Reliability Risks" (2016), available at https://www.brennancenter.org/analysis/fact-sheet-voting-system-security-and-reliability-risks; Norden and Vandewalker, "Securing Elections From Foreign Interference"; Haley Sweetland Edwards, "'Vote Flipping' Happens, but It Doesn't Mean the Election Is Rigged," *Time*, October 27, 2016, available at http://time.com/4547594/vote-flipping-election-rigged/.

54. Lawrence Norden and Christopher Famighetti, "America's Voting Machines at Risk" (Washington: Brennan Center for Justice, 2015), available at https://www.brennancenter.org/publication/americas-voting-machines-risk.

55. J. Alex Halderman, Testimony before the U.S. Senate Select Committee on Intelligence, "Russian interference in the 2016 U.S. elections," June 21, 2017, available at https://www.intelligence.senate.gov/sites/default/files/documents/os-ahalderman-062117.pdf.

56. Open Source Election Technology Institute, "Critical Democracy Infrastructure."

57. See, generally, Bagga, Losco, and Scheele, "Pre-Election Logic and Accuracy Testing and Post-Election Audit Initiative."

58. Additional, non-graded information is indicated by gray font throughout the report.

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, CrowdStrike, Inc. (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through your DocuSign, Inc. (DocuSign) Express user account. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to these terms and conditions, please confirm your agreement by clicking the 'I agree' button at the bottom of this document.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. For such copies, as long as you are an authorized user of the DocuSign system you will have the ability to download and print any documents we send to you through your DocuSign user account for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. To indicate to us that you are changing your mind, you must withdraw your consent using the DocuSign 'Withdraw Consent' form on the signing page of your DocuSign account. This will indicate to us that you have withdrawn your consent to receive required notices and disclosures electronically from us and you will no longer be able to use your DocuSign Express user account to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through your DocuSign user account all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact CrowdStrike, Inc.:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:

To contact us by email send messages to: tiffany@crowdstrike.com

To advise CrowdStrike, Inc. of your new e-mail address

To let us know of a change in your e-mail address where we should send notices and disclosures electronically to you, you must send an email message to us at tiffany@crowdstrike.com and in the body of such request you must state: your previous e-mail address, your new e-mail address. We do not require any other information from you to change your email address..

In addition, you must notify DocuSign, Inc to arrange for your new email address to be reflected in your DocuSign account by following the process for changing e-mail in DocuSign.

To request paper copies from CrowdStrike, Inc.

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an e-mail to tiffany@crowdstrike.com and in the body of such request you must state your e-mail address, full name, US Postal address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with CrowdStrike, Inc.

To inform us that you no longer want to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your DocuSign account, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an e-mail to tiffany@crowdstrike.com and in the body of such request you must state your e-mail, full name, IS Postal Address, telephone number, and account number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

Operating Systems:	Windows2000? or WindowsXP?
Browsers (for SENDERS):	Internet Explorer 6.0? or above
Browsers (for SIGNERS):	Internet Explorer 6.0?, Mozilla FireFox 1.0, NetScape 7.2 (or above)
Email:	Access to a valid email account
Screen Resolution:	800 x 600 minimum
Enabled Security Settings:	• Allow per session cookies • Users accessing the internet behind a Proxy Server must enable HTTP 1.1 settings via proxy connection

** These minimum requirements are subject to change. If these requirements change, we will provide you with an email message at the email address we have on file for you at that time providing you with the revised hardware and software requirements, at which time you will have the right to withdraw your consent.

Acknowledging your access and consent to receive materials electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please verify that you were able to read this electronic disclosure and that you also were able to print on paper or electronically save this page for your future reference and access or that

you were able to e-mail this disclosure and consent to an address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format on the terms and conditions described above, please let us know by clicking the 'I agree' button below.

By checking the 'I Agree' box, I confirm that:

- I can access and read this Electronic CONSENT TO ELECTRONIC RECEIPT OF ELECTRONIC RECORD AND SIGNATURE DISCLOSURES document; and
- I can print on paper the disclosure or save or send the disclosure to a place where I can print it, for future reference and access; and
- Until or unless I notify CrowdStrike, Inc. as described above, I consent to receive from exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by CrowdStrike, Inc. during the course of my relationship with you.

CENTER FOR
INTERNET SECURITY.

JOHN GILLIGAN
Chairman, Board of Directors

31 Tech Valley Drive, Suite 2 • East Greenbush, NY 12061
(518) 266-3460 • Fax: (518) 283-3216
john.gilligan@cisecurity.org

SECURING THE VOTE

Ill-Prepared States Invite Attack

EDITORIAL

❑ Valley News

VERMONT 5/13/18

ANDNEWHAMPSHIRE are each due to get about $3 million from the $380 million Congress appropriated in March to enhance election security. While not a huge amount, the money is welcome as all 50 states prepare for mid-term elections that will almost certainly be targeted by malicious hackers intent on creating chaos and undermining Americans' faith in elections.

Russian efforts to breach the voting systems of about 20 states during the 2016 election cycle have been documented by the Department of Homeland Security and the Senate Intelligence Committee, despite President Trump's efforts to cast doubt on whether Russian meddling took place. No evidence has been produced suggesting that the hackers succeeded in altering vote tallies or tampering with voter registration information, but there's every reason to fear that the Russians are of the "if-at-first-you-don't-succeed, try,-try-again " school. In fact, the Russians' efforts in 2016 appeared to many experts to be a trial run for a much more extensive effort in the future. And they may not be alone. Homeland Security Secretary Kirstjen Nielsen felt obliged to warn a group of 80 foreign diplomats, including the Russian ambassador, in a closed-door meeting in March not to meddle in upcoming elections or they would face retaliation. Homeland Security is now conducting risk assessments for 17 states that have requested them, a process that needs to be accelerated and coupled with increased information-sharing with election officials across the country. A number of other states, fearful of federal intervention in a function that has historically been controlled by local and state governments, have turned to the private and nonprofit sectors for security expertise.

Last week *The New York Times* reported on the extensive efforts West Virginia has made to secure its election infrastructure. Mac Warner, the state's chief election official, told the *Times* that some county clerks wondered why so much emphasis was being placed on cybersecurity when "the Russians aren't going to attack us." His answer? In the digital age, any state that does not secure its election systems is inviting an attack.

In testimony prepared for a Senate Intelligence Committee hearing this spring, Vermont Secretary of State Jim Condos outlined the measures Vermont has taken to boost the security of its election systems, including physical and cybersecurity risk assessments and adoption in 2015 of a new election management platform that includes built-in security measures. He said that Vermont follows a number of acknowledged "best practices," including use of paper ballots; daily backup of the voter registration database; daily monitoring of traffic to the election website; blacklisting of known or suspected problem IP addresses; and penetration testing. With the new money, Condos said later, "We will look at how we can ramp up even more security. We'll look at maybe beefing up our firewalls."

New Hampshire Secretary of State Bill Gardner was considerably less forthcoming when the *Concord Monitor* inquired about his plans for using the Granite State's share of the cybersecurity funds. He argues that the state's antiquated election technology is precisely what keeps its paper-based system secure.

Gardner's office also declined to provide information about its security measures to the Center for American Progress, a left-leaning think tank that compiled a detailed state-by-state election security report card that it released in February. Both New Hampshire and Vermont received a "C" (no state got above a "B"). The report card noted that while Vermont does indeed adhere to a number of "best practices," it needs to strengthen its post-election audit verification procedures, a fault it also found with New Hampshire. Condos toldWCAX that he disagreed with some of the report card's conclusions and had confidence in the state's system. But he noted that there's no room for complacency, as digital defenses must be constantly upgraded. "The bad actors have one way of doing it yesterday, a new way to do it today and a new way to attack tomorrow," he said. It's anybody's guess whether Gardner is taking cybersecurity seriously enough or whether he is still preoccupied with the chimera of "voter fraud." He claimed that his decision to join President Trump's spurious and now-deceased election integrity commission was motivated by a desire to restore people's faith in democratic elections. If so, he ought to take the occasion now to publicly explain what steps he is taking to counter an actual, known and widely acknowledged threat to election security.

It's anybody's guess whether

New Hampshire Secretary of State Bill Gardner is taking cybersecurity seriously enough.

Why I choose to arm myself

"(a)ll persons have the right to keep and bear arms in defense of themselves, their families, their property, and the state." - Part I, Article 2-a of the New Hampshire Constitution

Recently, I wrote an article on the need for a real conversation on firearms, the Second Amendment, and their place in "civil society" (https://bit.ly/2Ihv7lq). As expected I received several emails that offered suggestions as to how I might approach this conversation. Some helpful, some not so much. A conversation such as this requires focus, respect and patience, which is why I waited to write this series of columns away from the heat of the moment, while spreading the thought process over several articles.

As with most issues, it is important to be definitive when determining the end goal of a conversation, and we are far better off dissecting the conversation into small, well-defined tracks that lead us to that end goal. My goal for this conversation is simple: to eliminate the illegal use of firearms. That may not be your goal, or you may have different ideas on this topic. However, if this is a goal you can agree with, then we are already halfway there.

When I need to approach a conversation in the effort to build consensus (not necessarily total agreement), I find myself using a method some of you may be familiar with, the 6 Ws: Who, What, When, Where, Why and How.

When we discuss firearms in America, the 6W method is extremely helpful. Questions include who should be allowed to possess a firearm; what kind of firearms should be available; where should firearms be allowed to be carried; what is government's role in the possession of firearms; what is an individual's responsibility as a firearms owner; what kind of firearms should be legal and how do we prevent gun violence?

There are many more questions that can be added to this topic, and many would be similar in nature, just asked differently. However, surrounding all these questions is the most important W, the word why. The biggest why is "why do people own firearms?"

I cannot speak for all firearms owners, but I can for myself.

When you meet me, you can be certain of two things. I am both gracious and armed. The degree to which I may be armed will vary depending on the situation, but my graciousness knows no bounds. Some of you might be taken aback, perplexed either by the fact I believe myself to be gracious, but more likely because I state without reservation that I am committed to my own selfdefense. Some may ask why I feel the need to carry weapon. That is a great first question when we commit ourselves to a rational conversation on firearms. Who owns a firearm and why they choose to exercise the right of self-defense will surprise many who choose not to be armed.

Too often we only seem to talk about those among us who use guns in a criminal manner, and it is fair conversation to have, but it is only a small part of the equation. Every day you pass by law-abiding citizens who are armed and you don't even know it. Each of us is ordained with certain natural rights. Chief among these is the right to life and one's ability to defend themselves. No reasonable person would argue a law-abiding person should be denied the right to their own self-defense.

That defense will vary greatly based on numerous factors.

Should you choose not to possess a firearm, or other instruments that may aid in your survival, that is your right. But if you have not planned and prepared as to how you would handle a violent encounter, you have already labeled yourself a victim. And if that plan is to wait for the police, you have already lost. The police are under no obligation to protect you, and even the best police response will not be quick enough to prevent you from being victimized. Ask any police officer (off the record), and most will say they have never responded to the pre-scene of a crime. If that were not a true statement, the adage "there is never a cop around when you need one" would not be part of our lexicon.

I don't hunt, nor am I part of a biathlon team. I am neither interested in Bambi or a gold medal. I am concerned with one simple fact, the safety of my family, friends and my community. I have a firearm (as well as other self-defense tools) for one reason only: to protect my safety and that of those around me, including you. That is it. I do not have an inferiority complex, nor am I not paranoid. This juvenile approach to this conversation only makes you look foolish and ill-prepared for a serious conversation on not just firearms, but the larger discussion on violence and self-defense.

What I do possess is an absolute clarity of the world we live in. It is a world filled will decent, trusting people. It is also a world with just enough bad people for us as a society to always be vigilant. This is not a new epidemic, but a constant condition of mankind.

My possessing arms in the defense of my family in no way impedes on your freedoms. The illegal application of an instrument such as a gun, knife, car, computer to inflict harm on another provides us the opportunity as a culture to construct laws that address the offenders, while respecting a person's right to self-defense and privacy.

In my next few articles we will explore more of the 6 Ws related to firearms. *Jeff Chidester was raised in Portsmouth and is a lifelong resident of New Hampshire. He is radio host and political analyst for iHeart Radio – NH, which can be heard on Hampshire's News/ Talk Network: WQSO - 96.7 FM and New WGIR - 610 AM. You can find out more about Jeff by going to www.jeffchidester. com and you can email him at nhperspective@gmail.com.*

Foster's
5/13/18