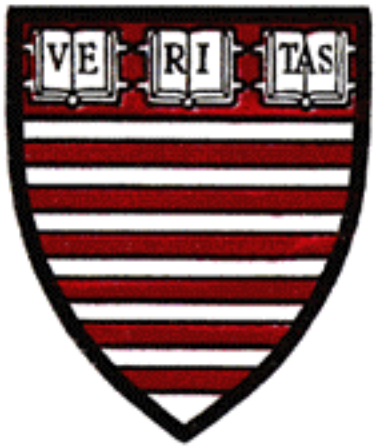
HARVARD UNIVERSITY
JOHN F. KENNEDY SCHOOL OF GOVERNMENT
Robert and Renée Belfer Center for Science and International Affairs



79 John F. Kennedy Street
Cambridge, MA 02138
tel: 617-496-6099
fax: 617-495-1905

To: interested Parties
Re: Proposal for Bipartisan Political Information Sharing And Analysis Organization
Date: July 29, 2017

OVERVIEW

Given that foreign-sponsored hacking has affected candidates and campaigns in both parties over the last decade, Republicans and Democrats need to set high standards for cyber security, build better

infrastructure to prevent further attacks and manage incident response when attacks happen. Private sector industry groups have established non-profit information sharing and analysis organizations (ISAOs) that help member companies to coordinate security, share threat information, and interface with the government. The Belfer Center's Project to Defend Digital Democracy, co-led by Matt Rhoades and Robby Mook, is seeking to organize a bipartisan version of the ISAO model for campaigns and political parties, in service of its overall mission to better secure our democracy against outside attacks.

A lack of clear standards, access to technology, expertise, and threat awareness has emerged as a serious vulnerability for all campaigns and political parties. The organization proposed in this memo would carry out many of the functions of a traditional ISAO, but could go further, to be a resource for in-kinded security technology, training, incident response, and advocacy with industry and federal officials.

SCOPE

Information Sharing

This organization will be responsible for coordinating information sharing and threat intelligence and analysis between campaigns, industry and government. Today, campaigns and political committees have no routine method for communicating with major platforms and service providers about incoming threats; this organization would create a one stop shop for campaigns and providers to keep each other informed. This organization will also be responsible for facilitating as much intelligence sharing and coordination as possible between campaigns/ parties, law enforcement and the Department of Homeland Security.

Standards, Playbook and Training

A lack of clear cybersecurity standards for parties, committees and candidates has been slowing efforts to better secure our political and civic space. Setting these minimum standards should be a top priority for this organization. In order to set and implement these standards, the organization could do five things:

1. Establish and educate members on cybersecurity standards for campaigns and parties that are kept current with threat intelligence, industry best practices, and legal compliance.

2. Create a "playbook" for campaigns and parties that is accessible to campaign professionals and adapts to the different sizes and functions of state/local/national campaigns and parties.

3. Create training materials or curricula that campaigns can use to train staff on security awareness and/or conduct onsite trainings themselves.

4. Create special training materials and curriculum for candidates, elected officials, and their families on how to secure themselves.

5. Seek ad advisory opinion from the FEC to in-kind professional training and development from industry to campaigns and political staff (CISSP, etc.).

Response

When intelligence indicates that a breach and/or information operation is underway or likely, the organization can partner with the private sector and government to help the campaign or party to respond.

Security Products and Services
The organization will seek ad advisory opinion from the FEC to in-kind products and services from industry. This will include security technologies, consulting, training, and auditing/certifying the security of campaigns and parties.

Auditing Vendors
Ideally, this organization could provide a service to audit and certify the security practices of political vendors, especially those that have access to sensitive strategic information.

Incident analysis and public
The organization could do forensic analysis of known breaches and information operations and release findings consistent with the organization's bylaws and with the permission of affected parties. The organization could potentially be a way to educate the media about the nature of an incident.

GOVERNANCE

Oversight
An oversight board of stakeholders from parties and campaigns should be established to help set priorities. What structure this board should take and who should participate can be determined as the exact form and objectives of the organization are determined.

Some ISACs lack relevance to their constituents because they're too dominated by vendor marketing and don't add enough direct value to their "customers". It will be essential that this organization be governed by the campaigns and parties themselves and focused on providing meaningful training and support.

Technical Advisory Board

A board of technical experts should help set the organization's objectives, systems, and recruit top level staff, starting with the Executive Director. Members should represent the best talent from government and the private sector. Representatives from the following entities are being considered for the advisory board.

- Former DHS and/or NSA personnel
- Jim Venebles, Chief Information Risk Officer, Goldman Sachs
- Jim Routh, Chief Security Officer, Aetna
- TBD Microsoft
- Alex Stamos, Chief Security Officer, Facebook
- Heather Adkins, Director of Information Security, Google
- Dmitri Alperovitch, CEO, Crowdstrike