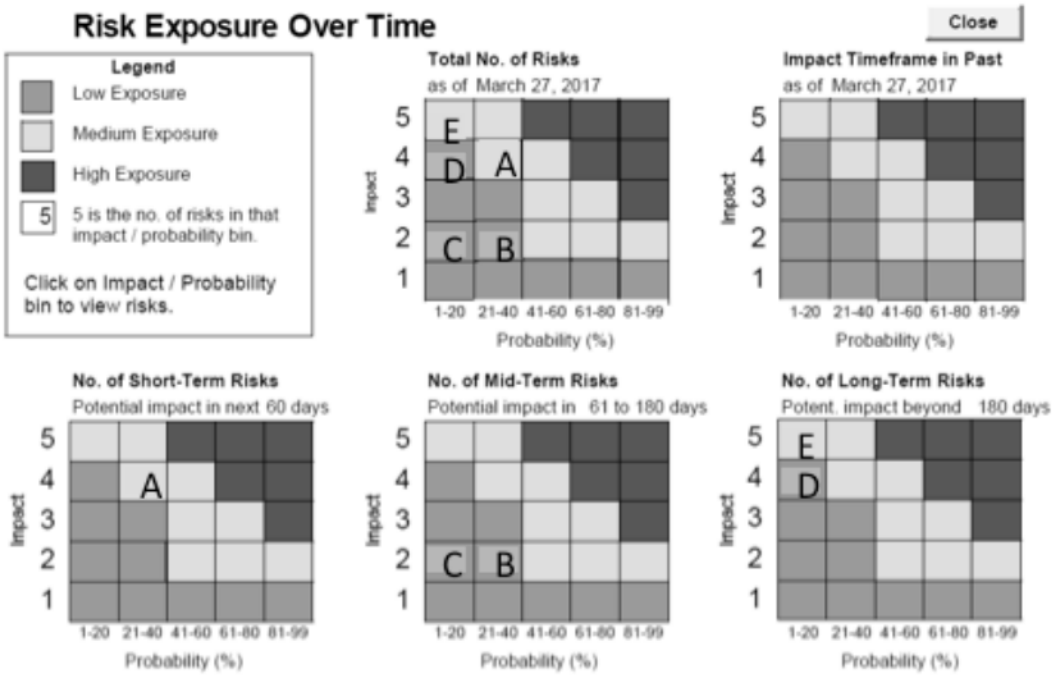
ACI R&D Risk Summary and Report



Risk I.D.	Risk Rank	Title	Probability %	Impact 1-5	Exposure	Impact Horizon	Control	Status
A	1	Test Article unsuitable for long term testing	30	4	1.2	Near	Internal	Watch
B	2	Insufficient resources to complete tests	25	2	0.5	Mid	Internal	Watch
C	3	Team members unable to perform all testing	20	2	0.4	Mid	Internal	Mitigate
D	4	Test reports do not identify any vulnerabilities	15	4	0.6	Far	Internal	Watch
E	5	Industry stakeholders attempt to suppress or invalidate results	20	5	1	Far	Internal	Watch

Summary: A risk analysis and report were completed for the Aviation Cyber Initiative Research and Development (ACI R&D) program. This report reflects possible program risks as they are understood to currently exist and will be updated as additional risks are uncovered.

Detailed Report: Risks by Rank **Aviation Cyber Initiative Research and Development**
Report Dated: Apr 10 2017

Risk ID A *Test Article unsuitable for long term testing* **Ranked** 1 **out of** 5 **risks**

Description: The ACI R&D requires a suitable test platform equipped to represent a majority of commercial aircraft currently in operation. To address the primary concern of the cyber analysis this test platform must be procured within the budget constraints currently available. This necessitated procuring an older B-757-200 that had reached end of life and is equipped with some older technologies no longer widely in service. For long term testing the test article must continue to represent technologies that are widely in use.

Probability: 30 (%) **Exposure** 1.2

Impact: 4(1=low, 5=high) (Prob. x Imp.; .01 = very low, 4.95 = very high)

Impact Time Frame: May 01 2016 **to:** Sep 30 2018

Impact Horizon: Near **Critical Path:** Yes

Date Identified: May 2016

Responsible Person: PM

Program Area: Penetration Testing

Affected Phase: All Phases

Risk Area: Cost. In order to upgrade aircraft components as required to meet long term testing requirements, the costs to upgrade and replace may exceed budget limits, limiting a test article's usefulness.

Control: Internal. Develop multi-year plan that takes into account upgrade requirements that provide the most benefit vs. cost. Schedule tests to reflect requirements that can be met by current test article.

Current Status: Mitigate. Develop appropriate cost plans to diversify exposure to a single test article.

Contingency Plan

Engage various stakeholders to allow for alternative testing plans as the program continues testing plans for 2017/2018. Begin to lay groundwork for procuring a suitable Airbus test article in order diversify systems to be tested.

Mitigation Plan

Exploring options other than procuring additional aircraft. Leasing the use of an aircraft is also viable path. Also continue to build out suitable lab facilities to test sub systems before adding to expense of installing newer systems onto the test article.

Detailed Report: Risks by Rank **Aviation Cyber Initiative Research and Development**
Report Dated: Apr 10 2017

Risk ID B *Insufficient Resources to complete all identified tests* **Ranked** 2 **out of** 5 **risks**

Description: DHS S&T has stated that cyber testing of aircraft is important to their mission, however the program does not have accurate requirement to address what is to be done when vulnerabilities are discovered. While all tests will follow the same process, budget estimates do not reflect the unknown complexity that may be discovered during the course of testing. This may lead to resource shortfall in completing all the desired testing within the timeframe outlined.

Probability: 25 (%) **Exposure** .50

Impact: 2(1=low, 5=high) (Prob. x Imp.; .01 = very low, 4.95 = very high)

Impact Time Frame: May 01 2016 **to:** Sep 30 2018

Impact Horizon: Mid **Critical Path:** No

Date Identified: Dec 16 2016

Responsible Person: PM

Program Area: Schedule

Affected Phase: Testing

Risk Area: Performance. Program has identified many tests to accomplish without clear knowledge of how the complexity of some systems will impact planned schedule performance

Control: Internal. Weekly status reports, peer reviewed test plans and a high degree of oversight will identify potential problem areas early when mitigation can still be successfully applied

Current Status: Watch

Contingency Plan

Prioritize high value testing and front-load that work so that it has the highest likelihood of completion. Schedule several milestone reviews and be prepared to suspend or shorten testing if it is forecast to significantly exceed schedule or costs unless a critical determination is being made.

Mitigation Plan

Include as many other stakeholders outside DHS as possible in order to grow group of agencies that are supporting this project. Be prepared to outsource some testing and continuously monitor on-going testing for relevance and appropriate findings.

Detailed Report: Risks by Rank **Aviation Cyber Initiative Research and Development**
Report Dated: Apr 10 2017

Risk ID C ***Assigned personnel unable to accomplish test goals*** **Ranked** 3 **out of** 5 **risks**

Description: The goal of the ACI R&D project is to demonstrate whether or not a cyber attack against a commercial aircraft is possible. It is important that the necessary personnel have the skills to investigate all viable cyber entry paths. The skillsets for technical performers capable of performing penetration tests against non-IT systems (flight management systems, radios, etc) are unique and not readily available. If the right technical skills are not brought to bear then, the test goals may not be fully accomplished.

Probability:20 (%) **Exposure** .80

Impact: 2(1=low, 5=high)(Prob. x Imp; .01 = very low, 4.95 = very high)

Impact Time Frame: May 01 2016 **to:** Sep 30 2018

Impact Horizon: Mid **Critical Path:** No

Date Identified: Aug 15 2016

Responsible Person: PM

Program Area: Program Management

Affected Phase: Initial Test Planning

Risk Area: Performance

Control: Internal & External

Current Status: Mitigate

Contingency Plan

Ensure that the Prime contractor has experience and has the ability to hire qualified candidates. Where appropriate engage qualified sub-contractors and ensure that Research Labs and Academia who have performed similar work are brought in to review, comment and as required, perform testing.

Mitigation Plan

In order to mitigate the chance that a single performer is unable to accomplish the testing goals, the program manager is engaging multiple performers using different contract activities to ensure there is no single point of failure. Two national labs, academia, as well as qualified prime and sub-contractor industry performers will be given testing responsibility and this will reduce the probability that unqualified personnel are brought into the testing.

Detailed Report: Risks by Rank **Aviation Cyber Initiative Research and Development**
Report Dated: Apr 10 2017

Risk ID D ***Test reports do not identify any vulnerabilities*** **Ranked** 4 **out of** 5 **risks**

Description: The goal of the ACI R&D project is to demonstrate whether or not a cyber attack against a commercial aircraft is possible. While early testing indicates that viable attack vectors exist that could impact flight operations, if no significant vulnerabilities are discovered in testing, the future of the program would be at risk.

Probability: 15 (%) **Exposure** 0.60

Impact: 4(1=low, 5=high) (Prob. x Imp.; .01 = very low, 4.95 = very high)

Impact Time Frame: May 01 2016 **to:** Sep 30 2018

Impact Horizon: Far **Critical Path:** No

Date Identified: Aug 15 2016

Responsible Person: PM

Program Area: Testing

Affected Phase: Phase 2

Risk Area: Performance

Control: Internal & External

Current Status: Mitigate

Contingency Plan

This risk is an extension of Risk C in that to ensure that any existing vulnerabilities are discovered as early in testing as possible, it is best to ensure that multiple performers are looking at multiple penetration attack vectors and not be reliant on a single methodology or process.

Mitigation Plan

By breaking down the test article into various sub-systems, multiple vulnerability areas may be investigated. Therefore if a single-subsystem does not have any associated vulnerabilities discovered, it does not risk the programs overall goal of identifying vulnerabilities related to the test article as a whole. This will help the team to diversify and research multiple avenues thereby increasing the likelihood that serious vulnerabilities are discovered and understood.

Detailed Report: Risks by Rank **Aviation Cyber Initiative Research and Development**
Report Dated: Apr 10 2017

Risk ID E ***Industry Stakeholders attempt to suppress or invalidate test results*** **Ranked** 5 **out of** 5 **risks**

Description: The goal of the ACI R&D project is to demonstrate whether or not a cyber attack against a commercial aircraft is possible. Due to the nature of this testing, any potential vulnerabilities discovered could have wide-ranging and significant economic impact to industry stakeholders to the aviation transportation community. There is risk in that if industry chooses not to recognize the importance or validity of the testing they could move to suppress or invalidate the test results that could render the program ineffective.

Probability: 20 (%) **Exposure** 1.0

Impact: 5(1=low, 5=high) (Prob. x Imp.; .01 = very low, 4.95 = very high)

Impact Time Frame: May 01 2016 **to:** Sep 30 2018

Impact Horizon: Far **Critical Path:** No

Date Identified: 1 March 2017

Responsible Person: All Program Participants

Program Area: All Areas

Affected Phase: All Phases

Risk Area: Performance: Testing results must be valid and repeatable with no bias

Control: Internal & External: Consistent messaging across DHS is necessary

Current Status: Mitigate

Contingency Plan: Develop effective communication strategy to ensure that accurate message on testing results is developed. Hold frequent stakeholder meetings to communicate current activity. Avoid making recommendations without the underlying data; do not inject policy discussion into test reports.

Mitigation Plan: Develop strong communication network to distribute test plans and resultant test reports. Engage with industry to ensure appropriate messages are being communicated. To maximum extent possible keep work unclassified in order to share information easily. Develop wide network of performers to demonstrate lack of bias in reporting. Finally ensure that test reports are reviewed and the results are easily verifiable and repeatable.

Aircraft Systems Information Security Protection (ASISP) Research

NextGEN

March 21st 2017

Presented to
DHS - Technical Exchange Meeting
By Isidore Venetos
William J. Hughes Technical Center
Aviation Research Division (ANG-E2)
ASISP R&D Manager
Isidore.venetos@faa.gov

FAA

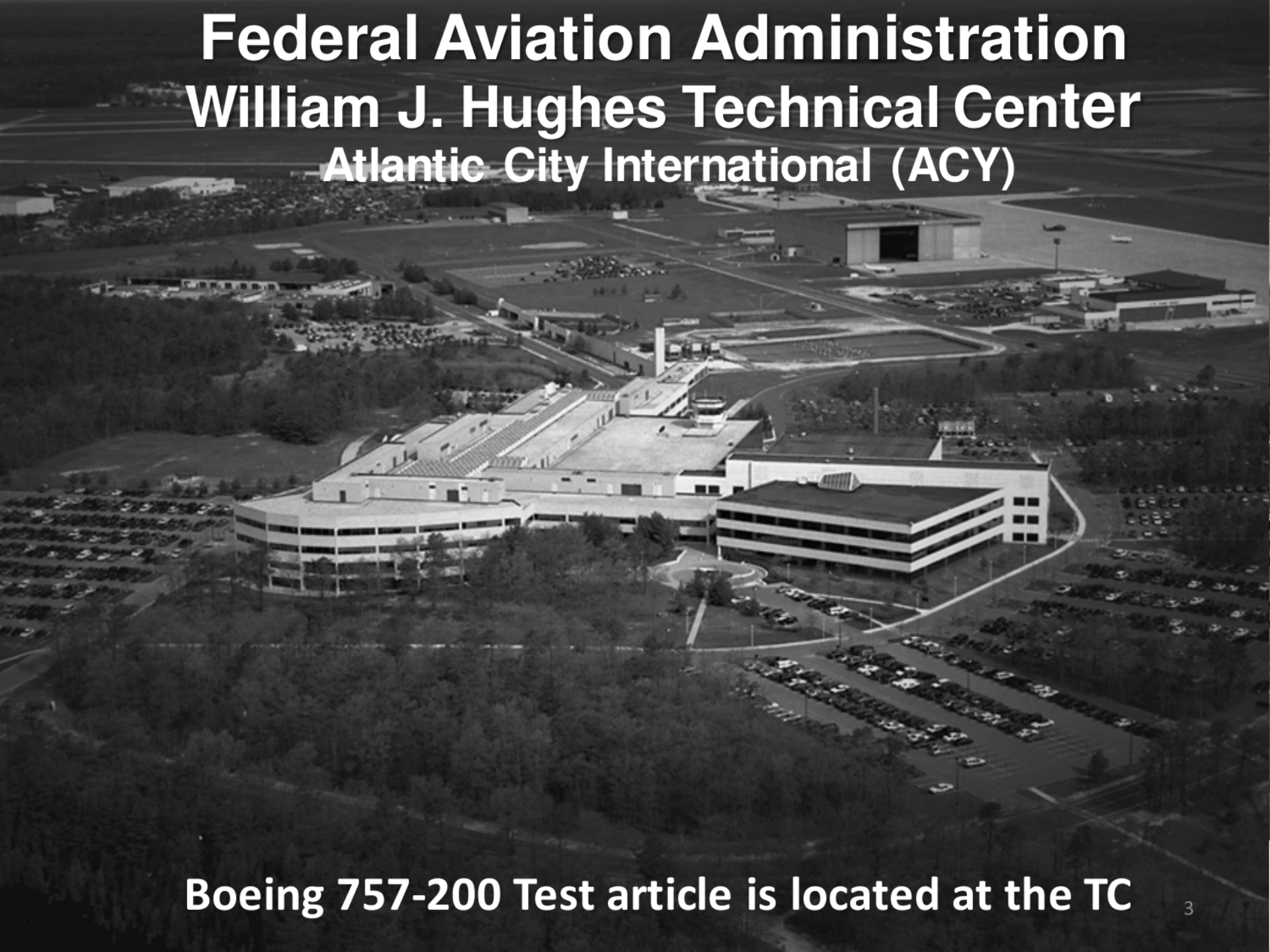
(b)(6)

Topic Review

✈ Today's objective: Present an Overview of FAA R&D for the **Aircraft System Information Security Protection** (ASISP) R&D effort which is focused on identifying Aircraft cyber risks

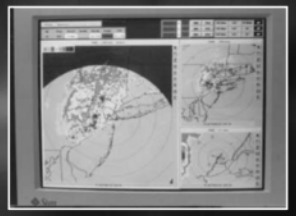
- FAA Technical Center Introduction
- FAA AVS Research Overview
- FAA AVS ASISP Requirement
- FAA ASISP R&D Framework
- DHS ACI–R&D Partnership
- FAA ASISP Partners

Federal Aviation Administration
William J. Hughes Technical Center
Atlantic City International (ACY)



Boeing 757-200 Test article is located at the TC

Technical Center: Multiple FAA Missions



Modeling and Simulation

Concept Development and Validation

Systems Engineering

Research & Development

Test and Evaluation

ACY Tower (ACM)

Engineering/Program Management

Laboratories

Center Operations

Flight Inspections

Safety

Operations Support

Aviation Safety (AVS) Organization Responsibilities

The FAA's Aviation Safety Organization is responsible for the certification, production approval, and continued airworthiness of aircraft as well as the certification of pilots, mechanics, and others in safety-related positions.

Aviation Safety is also responsible for:

- Certification of all operational and maintenance enterprises in domestic civil aviation
- Certification and safety oversight of approximately 7,300 U.S. commercial airlines and air operators
- Civil flight operations
- Developing regulations

FAA

OFFICES IN OVER **80** LOCATIONS

NEARLY **7,200** EMPLOYEES

USES NEARLY **10,000** DESIGNEES

Risk-Based Decision Making Sub-Initiatives and Activities

1 Improve standardization, data access, and modeling integration

- Taxonomies
- Modeling
- Greater data access
- Hazard tracking
- Safety data and risk analysis competencies and skills

2 Enhance decision making process

- Identify safety hazards of planned changes
- Identify and mitigate safety risk of existing cross organizational issues
- Changes to FAA SMS decision-making and governance structure

3 Evolve the Safety Oversight Model

- Leverage industry's use of safety management principles; exchange safety management lessons learned and best practices

Transition to Safety Management

- Operationalize the outputs of the RBDM activities
- Focus on conducting safety risk assessments on FAA Safety Issues and Planned Changes (on-demand)

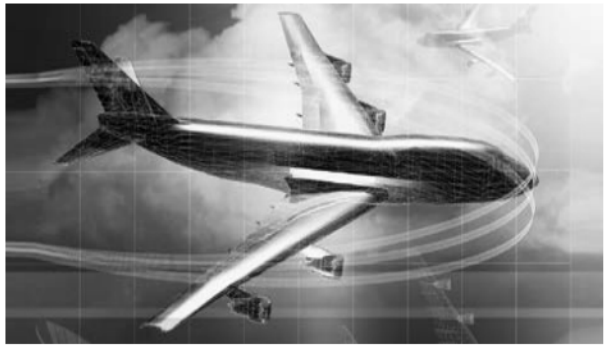
Aviation Safety (AVS) Organization Research and Development Activities

The primary purpose of AVS-sponsored research is to support the development of regulations, standards, and guidance materials needed to meet the FAA safety goals and objectives

Safety Events and Concerns Often Result in….

Aircraft Fire Issues

Propulsion Issues



Aircraft Cyber

Aircraft Structural Issues

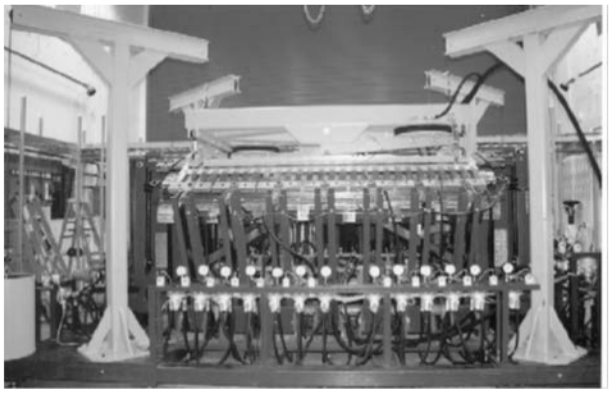
FAA

Aviation Safety (AVS) Organization Research and Development Activities

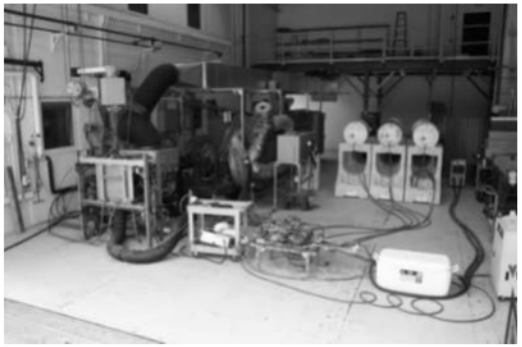
Research is to support the development of regulations, standards, and guidance materials needed to meet the FAA safety goals and objectives.

Aircraft Fire R&D

R&D generating supportive data for AVS policy & regulatory decision-making



Aircraft Structural R&D



Propulsion R&D

Aircraft Cyber R&D

FAA

Page 015 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

Page 019 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

Critical ASISP Partnerships

Private Sector & Academia

FAA & Aviation Community

International

Government Agencies

SC-216

SC-222

FAA

DHS

DOD

NASA

Cybercom

Page 023 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

Page 025 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

Page 026 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

Page 027 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

FAA

NextGEN

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by **Battelle** *Since 1965*

PNNL Results & Findings

PNNL Agenda

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- The Mission
- Mission Parameters and ROE
- Test Article
- Testing
- Results
- Implications
- Questions and Discussion

Why is this a Mission?

- Cyber defense of critical infrastructures/services is a national imperative
- The transportation sector is a part of the nation's critical infrastructure
  - Not physical infrastructure, also the vehicles
  - Cyber defense of a mobile platform (vehicle) is different than defending a fixed-in-place facility
  - Potential of catastrophic disaster is inherently greater in an airborne vehicle
  - A matter of time before a cyber security breach on an airline occurs
- It is essential that these elements be widely understood and acknowledged since effective cyber defense of aircraft will require:
  - Cooperation
  - Information sharing
  - Informed and updated regulation/certification

The ACI R&D Mission Phase 1

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Test the potential for non-cooperative cyber penetration of a commercial aircraft
  - Validated: establish actionable and unauthorized presence on one or more onboard systems
  - Disproved (partial): unable to penetrate via selected access vector
- Tests designed to assess aircraft cyber vulnerabilities on currently flying equipment and airframes in "operating" conditions
  - Operational systems in their operating environments
  - Not test benches, laboratory settings, or simulators
  - As close to actual flight conditions as safety allows

Mission Parameters

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Test article to be a representative commercial aircraft
- PNNL assigned “access points” aft of the cockpit
- Attack vector to originate from publicly accessible site (e.g., passenger seat, passenger terminal, etc.)
- “Weapon system” cannot raise undo suspicion (e.g. standard IT hardware that can be taken through airport security and used openly)
- No “insider” assistance or access (e.g., only standard passenger accesses)

Analysis of Alternatives

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- Passenger Wi-Fi
  - Internet services and/or onboard entertainment/information delivered by Wi-Fi
  - Widely available (available on identified test article)
- In-seat Power System – delivered by USB port
  - Becoming more widely available
  - USB connection not always an option
- Satellite Communications
  - Entertainment (e.g., Satellite TV, proprietary service, etc.)
  - Other communications via aircraft's satellite antenna
  - Availability and services vary (available on identified test article)

Selected Vector: Wi-Fi Internet & information distribution system

Rules of Engagement

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

- No testing without FAA personnel present
  - FAA engineering personnel were on board throughout test
  - Actions beyond initial recon require coordination and approval
- Unauthorized/non-cooperative access for purposes of recon allowed
- Data exfiltration allowed
- No modifying or tampering with any systems discovered or accessed
- No DOS attacks, potentially damaging attacks
- No penetration or attempted penetration that would impact any safety of flight system (e.g., data bus, avionics/electrical system, engines, etc.)

Page 036 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 037 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 038 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 039 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 040 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 041 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 042 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

Page 043 of 117

Withheld pursuant to exemption

(b)(7)(E)

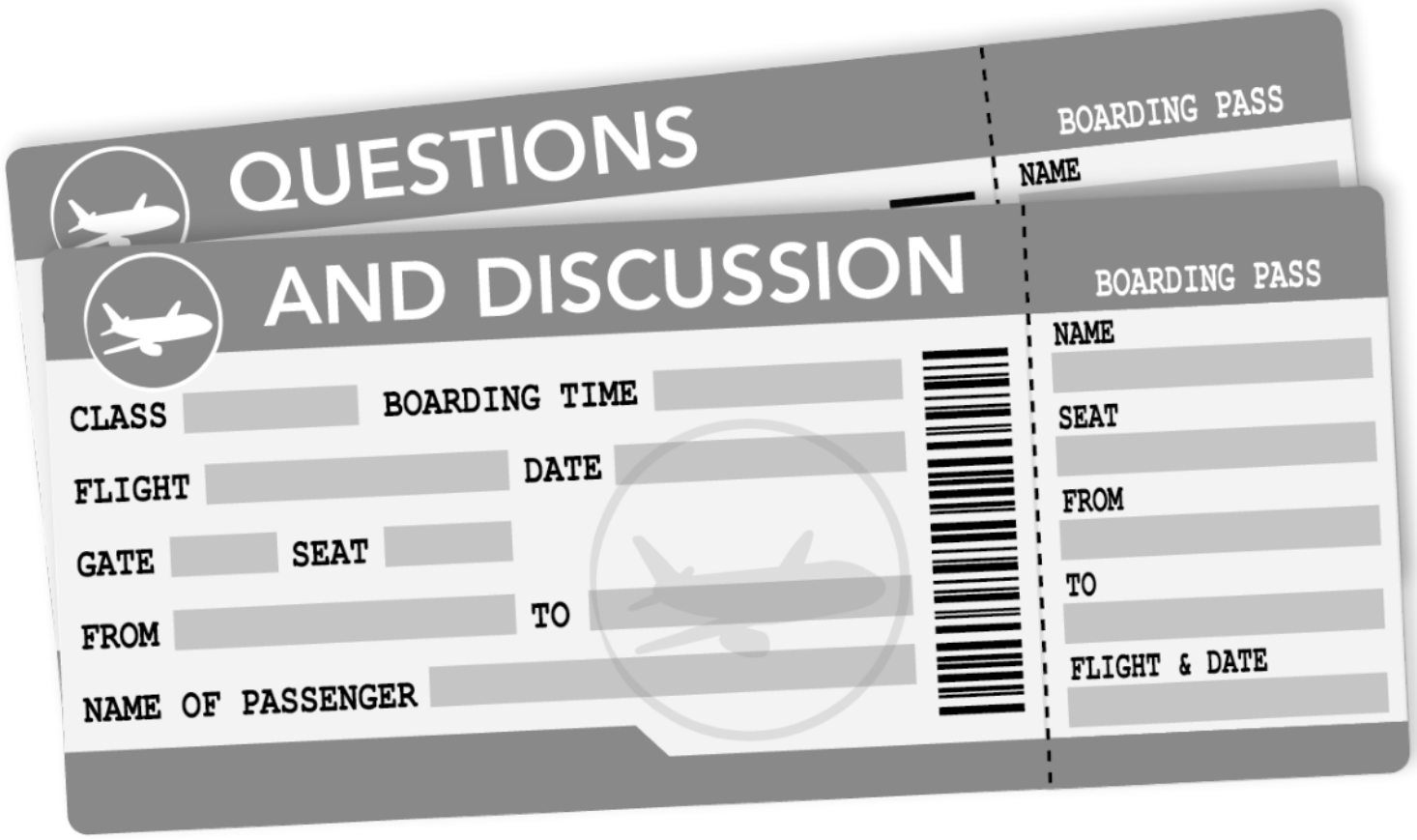
of the Freedom of Information and Privacy Act

PNNL PERSONNEL

Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by **Battelle** *Since 1965*

INDIVIDUALS

(b)(6)


QUESTIONS
BOARDING PASS
NAME
AND DISCUSSION
BOARDING PASS
CLASS
BOARDING TIME
FLIGHT
DATE
GATE
SEAT
FROM
TO
NAME OF PASSENGER
NAME
SEAT
FROM
TO
FLIGHT & DATE

Page 047 of 117

Withheld pursuant to exemption

(b)(4)

of the Freedom of Information and Privacy Act

Page 048 of 117

Withheld pursuant to exemption

(b)(4)

of the Freedom of Information and Privacy Act

Page 049 of 117

Withheld pursuant to exemption

(b)(4)

of the Freedom of Information and Privacy Act

Page 050 of 117

Withheld pursuant to exemption

(b)(4)

of the Freedom of Information and Privacy Act

Page 051 of 117

Withheld pursuant to exemption

(b)(4)

of the Freedom of Information and Privacy Act

Page 052 of 117

Withheld pursuant to exemption

(b)(4)

of the Freedom of Information and Privacy Act

Aircraft Cyber Evaluation (ACE)

ver. 8 (7.15.2016)

DHS Lead
Aviation Cyber Initiative (ACI)
Program Manager
Scott Buchanan
DHS/NPPD ICS-CERT

DHS Lead
Aircraft Cyber Evaluation (ACE)
Program Manager
Dr. Robert Hickey
DHS/S&T

Homeland Security

Problem Statement

- Today's commercial aviation backbone is built upon a network of trust; Most commercial aircraft currently in use have little to no cyber protections in place
  - Designed 25-30 years ago…safety and reliability
- A perceived successful cyber attack against a commercial aircraft could have far reaching and an enormous impact to the global aviation transportation industry
- Now more than ever exists a national imperative for interagency collaboration to understand, detect, and mitigate cyber vulnerabilities to commercial aircraft
- 2015 GAO report "FAA Needs a More comprehensive Approach to Address Cybersecurity as Agency Transitions to Next Gen"

In 2012, aviation accounted for 5.4% of our gross domestic product (GDP), contributed $1.5 trillion in total economic activity, and supported 11.8 million jobs. Aviation manufacturing also continues to be the nation's top net export.
FAA Report June 2014

Evolution of Cyber Threats to Aviation

1940's – 1980's
- Analog
- Cables & Hydraulics

1990's – Present
- 80% Trans-oceanic airlift now use Full Authority Digital Engine/Electronics Control (FADEC)
- Avionics Full-Duplex Switched Ethernet (AFDX)

In 10 -15 Years…
- Nearly all trans-oceanic airlift will be via FADEC equipped aircraft
- AFDX will be the industry standard for all commercial aircraft design
- Wireless communication for aircraft control and monitoring systems

(b)(7)(E)

Impact

Public Trust Impact

- Does not require "taking control" of an aircraft to impact public trust
- Create conditions that would cause a predictable action or response
- Cause Aircrew to deviate from planned activity
- Create conditions where public perceives there is risk to aircraft operations

Economic Impact

- Aviation transportation industry susceptible to even short term disruption
- Global economic health tied to affordable commercial aviation transportation
- Airline industry directly affects business and leisure travel economies
- Air cargo, for both commercial and military Ops will be affected

Tangential Impact

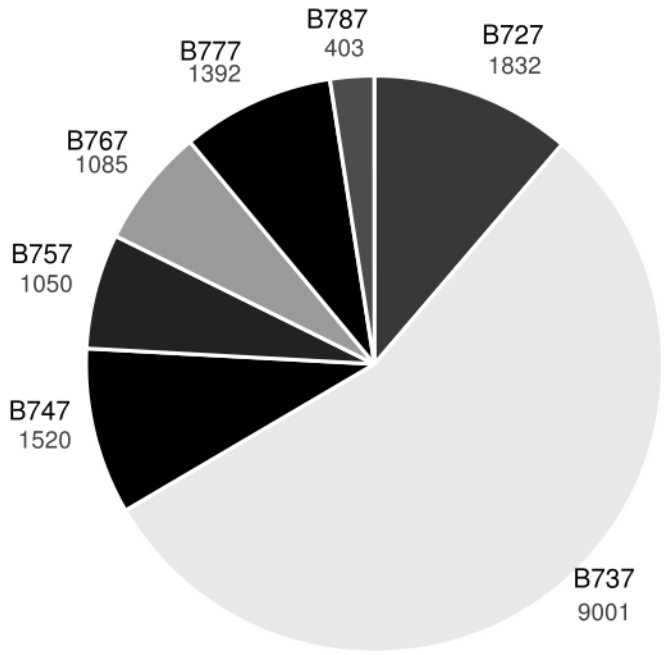
- Aviation Insurance costs driven by risk
- Aviation manufacturing leading U.S. export
- Effect on competitor if single airline is targeted
- Increase cost of doing business across numerous sectors
- Significant military use of commercial transport introduces national security risks

Action

DHS S&T has established the Aircraft Cyber Evaluation (ACE) project with the expressed purpose of evaluating the assertion that a cyber-attack via non-cooperative penetration is possible, and if so, provide recommendations and mitigation strategies to DHS leaders to address this possible risk:

- Conduct an evaluation and provide the results and findings
- Conduct a gap analysis to determine what cyber entry vectors should be evaluated
- Define and validate penetration test requirements
- Conduct test and evaluations
- Develop and publish the evaluation results and findings
- Support the development of a technical community that can address this infrastructure area

Boeing commercial aircraft built as of April 2016



- 2% of the Boeing aircraft are eEnabled
- 98% of the Boeing aircraft flying today are legacy aircraft (not eEnabled)
- Boeing estimates 20+ year service life for current aircraft deliveries of all models of aircraft (15-20 more years of higher cyber vulnerability)

In years 2010-2016 90% of Boeing aircraft delivered were NOT e-enabled.
These aircraft will continue to be in service beyond year 2030

Scope and Objectives

Scope: To evaluate the assertion that a cyber-attack via non-cooperative penetration is possible via specified attack vectors

(b)(7)(F)

Objectives:

- Gather and review previous cyber aircraft studies and activities that have direct applicability (create the baseline)
- Develop realistic operational test protocols
- Obtain the test element
- Conduct an operational test
- Create the results and findings report

Stakeholders and Partners

- DHS has stood up and is leading a multi-Agency Team tasked to develop and conduct an aircraft cyber evaluation
  - *Evaluation team includes participants from FAA, USAF, ODNI, NAI2-O, National Labs and Industry*
  - *Foster a collaborative environment that promotes cooperation, information sharing and transparency*
  - *Significant interest expressed by TSA, FBI, COCOMs, IC, and industry in monitoring the process and results*
- DHS is partnering with the FAA to locate the test element at the William J. Hughes Technical Center, Atlantic City, NJ, and work in full partnership with the Technical Center on the ACE, and future vulnerability assessments

What we anticipate

- Definitive results that either prove or disprove the attack vector and accessibility to critical aircraft systems
- Strategic planning to address long term response to cyber threats to transportation domain
- Anticipate significant reluctance by the commercial world to expend resources to prevent penetration & attack
  - USAF/USN data = detractor, “that’s unique to military aircraft”
  - Lab results = detractor, “you all did that in a lab, it couldn’t happen to my airplanes in the wild”
  - DHS data = independent test, open source information
- Continue outreach

Schedule and Deliverables

- **Schedule**
  - Procure the test element (ASAP, anticipated test element availability Aug 2016)
  - Develop test protocols (Jul 2016)
  - Conduct actual testing (Aug 2016)
  - Gather test results and findings and publish report (Sep 2016/FY17Q1)
- **Deliverables**

  Test Report
  - Initially 3 attack vectors planned (external RF, passenger onboard, and Maintenance and Supply Chain)—reduced to 2 attack vectors (RF and In-flight Entertainment)
  - MIT/Lincoln Labs – External RF
  - Pacific Northwest National Labs = WiFi/IFE/etc

  Strategic Communications Plan
  - Communications plan and message that will address this national imperative to various audiences in a manner that will not create unnecessary fear and or panic

Future Options

- FY 17 begin a comprehensive nose to tail vulnerability assessment of various aircraft systems (ACARS, FADEC, SATCOM, etc.)
- Develop mitigation strategies to deal with discovered vulnerabilities
- Work with Inter-Agency partners to address necessary policy changes and/or regulatory changes
- Explore the synergies of surface, maritime, and aviation cyber vulnerabilities and mitigations
- Create a separate communications plan to articulate these results to various audiences
- Develop structure to deal with transportation cyber vulnerabilities

Questions

BACKUP

Back-up stats

Airplane model series	Initial service	Number of active (total)* commercial fleet		Minimum design service objectives~	No. of airplanes exceeding 100% of minimum design service objectives
		Operators	Airplanes		
707	1958	26	46 (734)	20,000 flights 60,000 hours 20 years	3 25 46
720	1960	0	0 (153)	30,000 flights 60,000 hours 20 years	0 0 0
727	1964	116	1,142 (1,822)	60,000 flights 50,000 hours 20 years	14 730 767
737	1968	222	2,906 (3,216)	75,000 flights 51,000 hours 20 years	28 342 321
747^	1970	54	967 (1,178)	20,000 flights 60,000 hours 20 years	95 431 189
767	1982	68	711 (724)	50,000 flights 50,000 hours 20 years	0 93 0
777	1995	21	178 (0)	40,000 flights 60,000 hours 20 years	0 0 0

Source: http://www.boeing.com/commercial/aeromagazine/aero_07/corrosn_sb_table01.html

737 - 2831
747 - 108
767 - 106
777 - 576
787 - 431

Boeing Deliveries by Model 2010-2016

	707	717	727	737	747	757	767	777	787	DC-8	DC-9	DC-10	MD-11	MD-80	MD-90	Total
2010	-	-	-	376	-	-	12	74	-	-	-	-	-	-	-	462
2011	-	-	-	372	9	-	20	73	3	-	-	-	-	-	-	477
2012	-	-	-	415	31	-	26	83	46	-	-	-	-	-	-	601
2013	-	-	-	440	24	-	21	98	65	-	-	-	-	-	-	648
2014	-	-	-	485	19	-	6	99	114	-	-	-	-	-	-	723
2015	-	-	-	495	18	-	16	98	135	-	-	-	-	-	-	762
2016	-	-	-	248	3	-	5	51	68	-	-	-	-	-	-	375

Source: http://www.boeing.com/commercial/#/orders-deliveries

Process

- **The team that conducts the risk assessment must first collect system-related information, which is usually classified as follows:**
  - Hardware
  - Software System interfaces (e.g., internal and external connectivity)
  - Data and information
  - Persons who support and use the IT system
  - System Mission
  - System and data criticality
  - System and data sensitivity

DHS Science and Technology Directorate

Aviation Security: Aviation Cyber Initiative Research & Development

Securing America's Aircraft

S&T established a program to evaluate the assertion that a remote cyber-attack against commercial aircraft via non-cooperative penetration is possible, and if so, provide recommendations to DHS and interagency leaders for longer-term program objectives to address this risk. This S&T program supports the larger S&T and DHS mission of understanding, assessing and responding to cyber threats to critical infrastructure.

To meet this challenge, S&T is using an inter-agency approach that can extend through the Future Years Homeland Security Program (FYHSP). During FY16, the S&T program team acquired an Aircraft Test Article (TA) and conducted initial planning and evaluation, including:

1. Conduct a gap analysis to determine what cyber entry vectors should be evaluated
2. Define and validate penetration test requirements
3. Conduct initial evaluations
4. Develop and publish the evaluation results and findings
5. Support the development of a technical community that can address mitigation strategies in this infrastructure area.

The FY16 baseline remote, non-cooperative cyber penetration of the Test Article was successful. Building on this, in FY17-21 S&T will conduct a "nose to tail" systems vulnerability assessment and develop mitigation recommendations. Furthermore, S&T will partner with key government and industry stakeholders to improve acquisition methodologies to minimize cyber vulnerabilities to the Aviation transportation ecosystem.

Currently scheduled (FY17-18) aircraft system vulnerability assessments include: the Flight Management System, the aircraft electrical system, the Full Authority Digital Electronic Control (throttle to the engines), special cases mitigation (details classified), aircraft telemetry study, environmental and life support system, aircraft power plant/engines, autopilot/auto landing system, aircraft fuel system, primary flight display system, aircraft weight on wheels system, and the electronic flight bag vulnerability study.

S&T aircraft cyber vulnerability assessments support three of the five DHS Missions (Prevent Terrorism and Enhance Security, Safeguard and Secure Cyberspace, and Strengthen National Preparedness and Resilience), and four of the five DHS S&T Visionary Goals (a Trusted Cyber Future, Enable the Decision Maker, Responder of the Future, and Resilient Communities).

DHS Science and Technology Directorate

Aviation Security: Aviation Cyber Initiative Research & Development

Providing Education and Resources

Many pilots, mechanics and operations staff do not understand the nature and implications of a cyberattack on an aircraft. S&T is working with the FAA and other stakeholder partners to develop training and procedures that would help them understand that an un-recognized (or recognized) aircraft event could be the result of a cyberattack as opposed to an aircraft mechanical issue.

Multifunctional displays

Additionally, research, both within S&T and the results and findings from other research sources are uncovering the gap that current approaches to cyber security do not address the complicated sophistication and system interdependency that is resident in aircraft. Furthermore, current policies and practices are inadequate to deal with the immediacy and devastating consequences that could result from a catastrophic cyber attack on an airborne commercial aircraft.

Finally, developing an Aircraft cyber event response option that can address both commercial aircraft and military/civilian aircraft derivatives is imperative. Current approaches to industrial control systems and terrestrial based information technology infrastructure is not designed to address the unique nature of the integrated aircraft systems, and Aircraft cyber forensics is nonexistent.

Research is needed to address FAA's Aircraft Systems Information Security / Protection (ASISP) risk, which includes aircraft certification and continued operational safety. The research will explore where ASISP-related threats and risks can compromise fail-safe mechanisms in the architecture, design, and operation of aircraft systems, including ASISP-related particular risks that might lead to common cause failures. All of these efforts increasingly will be conducted in partnership with the FAA.

CYBERSAT 17

SECURITY IN AEROSPACE

November 7-8 | Marriott Tyson's Corner | Tyson's Corner, VA

WWW.CYBERSATSUMMIT.COM

CYBERSAT17
SECURITY IN AEROSPACE

November 7-8 | Marriott Tyson's Corner | Tyson's Corner, VA

Dr. Robert Hickey

When You Can't Stop the Vehicle; You Must Stop the Threat

Introduction

- Aviation and aviation-related activity constitute 58.1M jobs globally
- 3.4% of the Global Gross Domestic Product
- $2.4 Trillion annual global impact
- 9-11 "…an inaugural event, the beginning of a radically new period…"
- Ramifications of a creditable cyber attack on a commercial aircraft

(2012). "Aviation: benefits beyond borders."
Mitchell, W. T. (2012). "Poetic Justice: 9-11 to now." Critical Inquiry **38**(2): 241-249.

Economic Reality

Most current data indicates U.S. civil aviation accounted for:

- $1.6 trillion in total annual economic activity
- Supported 10.6 million jobs – 8.5% of all U.S.
- Contributed 5.1% to the U.S. GDP
- Civil aircraft manufacturing top net U.S. export; $60 billion positive trade balance

Most current data indicates U.S. general aviation accounted for:

- $150 billion annual economic contribution
- 1.2 million jobs

Globally, each day more than $18.6 billion of goods travel by air; one-third of all trade by value

- $2.4 trillion global economic impact; 58 million jobs globally

5.1% of U.S. GDP…12 Million U.S. Jobs and 58 Million Jobs Globally!

Slide courtesy of the NAI2O

A Day in the Aviation Domain

Domestically

- 23,911 commercial flights
- 2.3 million passengers
- 7,000 planes in the sky at any given moment
- Generating $2.6 billion in economic activity

Military (*based on 3-month average*)

- Personnel – 1,769
- Cargo – 819 tons
- Off-loads – 87
- Planned sorties – 1,198
  - Airlift: 222; Refueling: 60; Training: 263; Other: 54

Internationally

- 93,000 commercial flights
- 8.4 million passengers
- 13,000 planes in the sky at any given moment
- Generating $7.4 billion in economic activity
- 59,466 commercial airports and civ/mil airports/airfields

Slide courtesy of the NAI2O

Today's Flight Plan

- Traditional Critical Infrastructure
- Other Types of Critical Infrastructure
- Protecting the Non Traditional Critical Infrastructure
- Aircraft and Cyber
- Protecting the Aircraft
- Conclusions

Traditional Critical Infrastructure

- 1998 President Bill Clinton signed Presidential Policy Directive PPD-63
- 2003 President George W. Bush signed Homeland Security Presidential Directive (HSPD) 7
- 2009 Cyberspace policy review led by Mr. Melissa Hathaway
- 2013 President Barack Obama signed Presidential Policy Directive 21
  - 16 Critical Infrastructure Sectors
    - Transportation

Traditional Critical Infrastructure did not consider NON-TRADITIONAL Critical Infrastructure

Clinton, W. J. (1998, May 22, 1998). "Protecting America's critical infrastructures: PDD 63." Presidential Decision Directive. from http://www.fas.org/irp/offdocs/pdd-63.htm.
Bush, G. W. (2003). "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection."
Obama, B. (2013). "Presidential Policy Directive 21 -- Critical Infrastructure Security and Resilience."

Other Types of Critical Infrastructure

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - NIST may not be appropriate for Other types of Critical Infrastructure—Infrastructure in motion
- Critical Infrastructure in motion
- Unique characteristic
  - The ongoing activity associated with surface transportation cyber security is a testimony to the thought that traditional methods may not be adequate (Markey 2015)
  - Locomotive designed to be in service for 25 years (Norfolk Southern 2014).
  - Aircraft require eight years from design to production

Markey, E. (2015). "Tracking & Hacking Security & Privacy Gaps Put American Drivers at Risk." 14.

Protecting Non Traditional Critical Infrastructure

- Shifting the paradigm for non traditional critical infrastructure
  - Focus on operational requirements, not perimeter defense
  - Not enough resources to protect everything
    - Identify the critical systems and components first and protect them
    - Protecting the legacy aircraft
- Understanding the environment
  - Understanding aviation intelligence as it pertains to cyber
    - Open source
    - Fusing data to develop the landscape
    - Must move the event further to the left, wheels in the wells, game over
  - Understanding the vulnerabilities (the threat)
    - We can only understand the vulnerabilities through diligent and deliberate research

An aircraft is not an IT System in the traditional sense. Current framework is not appropriate

Aircraft and Cyber

- Aircraft crashes and the subsequent investigations
- Majority of aircraft flying today were designed 30-40 years ago
  - Two tenants in the design—safety and reliability
  - 3.2% of the Boeing aircraft flying today were designed with some cyber in mind (B787)
- System design assumed trusted connections
  - No authentication
- Design complexity, years of maintenance modifications, remote access, & travel speed—unique mobile transportation infrastructure
- Trend toward the Internet of Things
- 3.4% Global—5.4% of the US GNP

…" the average age of a U.S. domestic commercial airliner is 11 years old, it is not uncommon for aircraft to still be in service at 24, 25, even 30 years old."
Bill de Decker – Conklin & de Decker Aviation

Protecting the Aircraft

- 9-11 Demonstrated a new weapon
- ORD scenario
- B-737 scenario
- WOW switch
- Oversimplification to categorize an aircraft as a traditional information technology system
- Not an "enterprise" network either, running MS Windows or Norton Anti-virus
  - Embedded systems, running custom operating systems with custom applications
- Trend is toward an Internet of Things (IoT)—WHY??

Conclusion

- **Conclusion:** A prolonged aviation industry disruption brought on by a perceived or actual cyber threat (or attack) on commercial aircraft would have serious economic consequences to the United States.
- **Conclusion:** Critical infrastructure, that is in motion (a vehicle), demands a paradigm shift from traditional methods of protecting and reconstituting stationary critical infrastructure.
- **Conclusion:** Sharing research results and findings is foundational to the required paradigm shift.
- **Conclusion:** Increased industry specific cyber education is required.
- **Conclusion:** Policy changes that are appropriate for the time, too long to make cyber changes on aircraft

NON TRADITIONAL Critical Infrastructure demands a new approach.
We will not solve tomorrow's problems with yesterday's solutions.

Get Off the Stage Slide

- What?
  - Cyber attack on commercial aircraft.
- So What?
  - We have to prevent the attack itself, well before it takes place.
- Now What?
  - Research and share results and findings
  - Education—both in operations and maintenance.
  - Policy

Program Execution & Tech Review

AIRCRAFT CYBER INITIATIVE RESEARCH AND DEVELOPMENT



Dr. Robert Hickey
Program Manager
Cyber Security Division
Science and Technology Directorate
April 2017

Homeland Security
Science and Technology

Program Execution & Tech Review Outline

1. Programmatic Introduction:
   - Problem Statement/Capability Need (Why)
   - Program Planning & Execution
   - AoA/Competition/Alternatives
   - Stakeholder Engagement

2. Technical Approach & Planning*
   - Program Technical Goals
   - Tech approach to meet those needs
     - SOW/Deliverables
     - Tech Challenges
     - Cost/schedule/performance implications of tech challenges
     - Tech Risks (e.g. obsolescence)
   - Achievements previous 12 months & Technical Impact
   - Overall R&D & Tech trends/advances relevant to your project

3. Other Program Information
   - Transition Planning: Prototyping, Experimentation, Testing & Evaluation, Transition Plan
   - Program Risk
   - Budget and Funding
   - Investment Benefit/Program Impact

Page 086 of 117

Withheld pursuant to exemption

(b)(7)(E)

of the Freedom of Information and Privacy Act

1.1 Programmatic Introduction (cont.)

- Stakeholder Engagement
  - DHS has appointed ICS-CERT as the overall governmental lead for the Aircraft Cyber Initiative (ACI)
    - S&T CSD will perform research to identify aviation critical infrastructure vulnerabilities.
  - Partnerships include: the TSA, FAA, the FBI and the DOD. National Labs, Academia and Industry partners will be included in testing as the need to coordinate and address vulnerabilities becomes appropriate.
    - These partners will work together to define specific areas of responsibility within the framework of activities to accomplish the objectives of this plan
  - Priority alignments between the works being conducted by the FAA Aviation Research Division (ANG-E2), Aircraft Systems Information Security Protection, Manager and ACI R&D have been evaluated.
    - The coordination of these two efforts (FAA ANG-E2 and DHS S&T) provides synergistic results in two areas: 1) coordination demonstrates interagency integration and coordination and 2) eliminates as much duplication potential as possible.

2.0 Technical Approach/Planning

- Program Technical Goals
  - The goal for FY17/18 are to clearly identify and articulate the various systems vulnerabilities and work with the inter-agency partnerships, academia, and industry to develop mitigation strategies and solutions to nullify the discovered vulnerabilities.
  - Deliverables will consist of test reports, studies, cyber tools and prototype mitigation technology to address defensive cyber capabilities.
- Technical challenges
  - Limitations of test article configuration may impact detailed analysis of some systems (Passenger Inflight Entertainment, Electronic Flight Bag, Primary Flight Display)
- Technical impact
  - Met all technical goals in FY2016
  - TEM held 21 March 17 provided 2017 technical goals to stakeholders
  - Delivered comprehensive ACARS test report
  - Successful testing resulting in policy impacts
  - Penetration testing resulting in community action. Industry impact
- R&D Trends/Other tech advances related to your program/project
  - In 2017 ACI R&D will begin shift from penetration testing to mitigation development. 2018 will begin to investigate e-enabled aircraft.

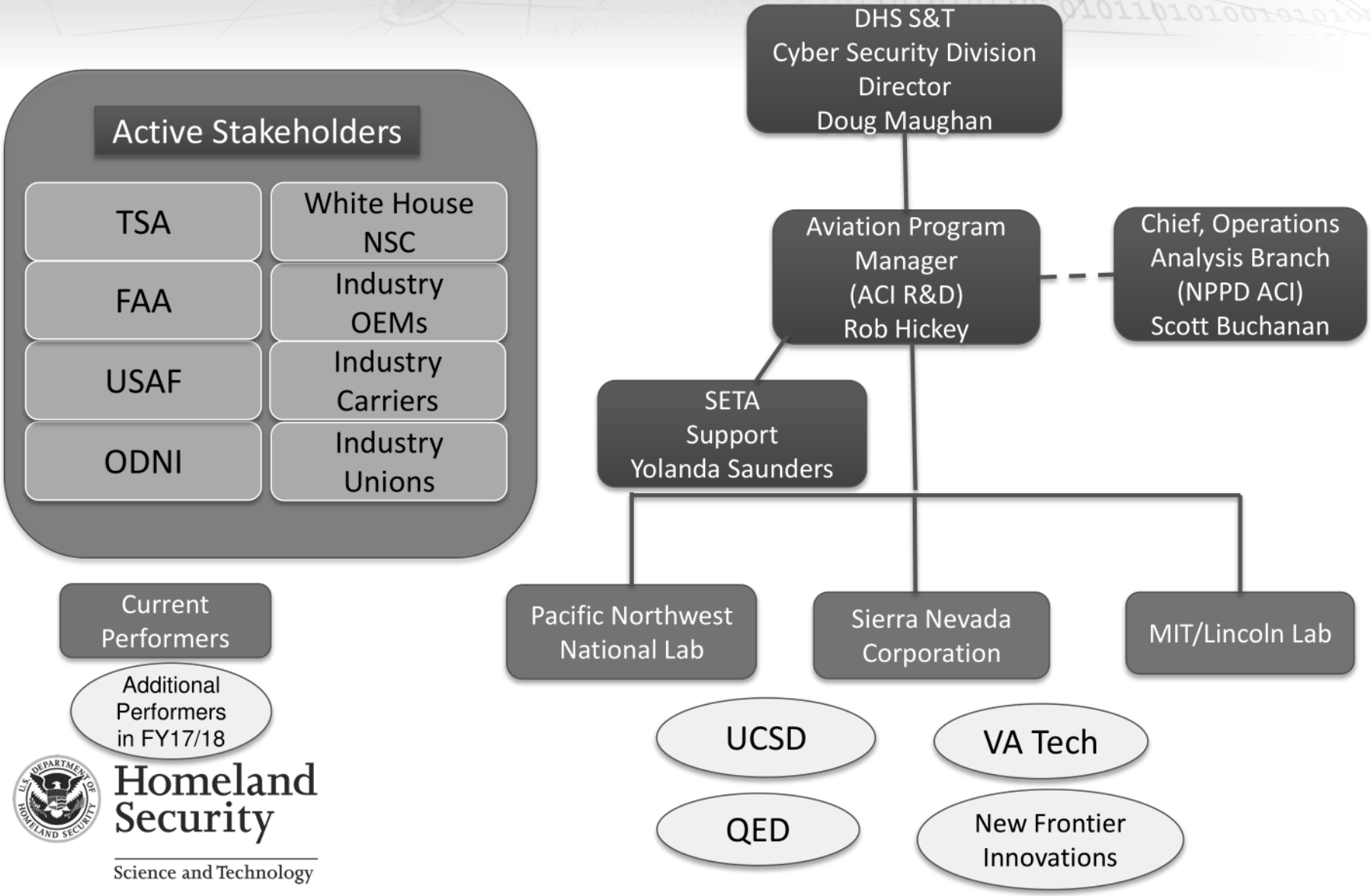
2.1 Master Schedule

Test	3rd Qtr. FY17	4th Qtr. FY17	1st Qtr. FY18	2nd Qtr. FY18
Technical Exchange Meeting				
FMS (Study 1)				
Electrical System (Study 2)				
FADEC (Study 3)				
Telemetry System (Study 4)				
Environmental/Life Support (Study 5)				
Engines (Study 6) / Fuel Systems (Study 8)				
Autopilot/Landing (Study 7)				
Electronic Flight Bag (Study 9)				
"Big Bird" Mitigation * (ACARS) (Study 10)				
A/C Cyber Field Team (Study 11)				
Primary Flight Display (PFD) (Study 12)				

Homeland Security

Science and Technology

3.0 Stakeholder Engagement / Organization Chart



Homeland Security

Science and Technology

4.0 Transition Planning: Prototyping, Experimentation, Transition Plans

- Hack-a-Thon (offensive/defensive)
  - Transition findings to FAA for possible industry regulation
- Partner with FAA to leverage S&T investments for risk analysis
- Collaboration with FAA to determine Safety of Flight (SoF)
  - Develop process for rapid transition of possible SoF findings
- Collaborate with Industry for non Safety of Flight issues
- Stakeholders are eager to receive help and are looking for solutions to solve their current gaps and threats through the Technical Exchange Meetings
  - Establish framework for technical information exchange with industry and other stakeholders

Page 092 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

Page 093 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

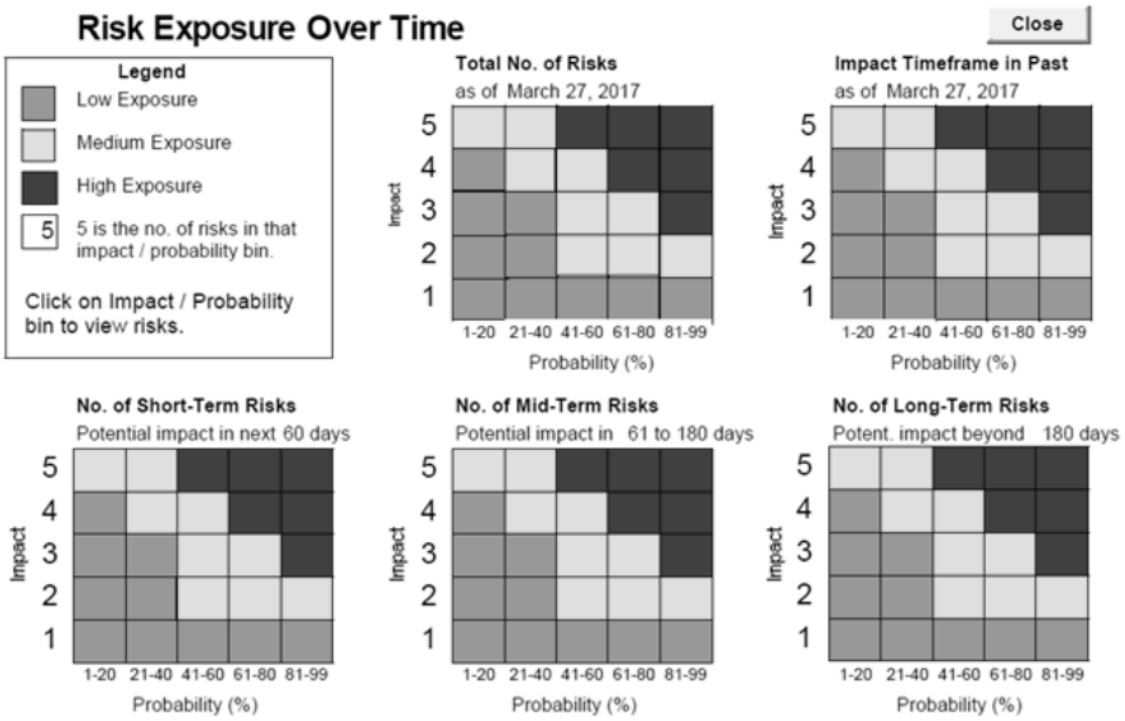
Page 094 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

6.0 Program Risk



Risk I.D.	Risk Rank	Title	Probability %	Impact 1-5	Exposure	Impact Horizon	Control	Status
A	1	Test Article unsuitable for long term testing	30	4	1.2	Near	Internal	Watch
B	2	Insufficient resources to complete tests	25	2	0.5	Mid	Internal	Watch
C	3	Team members unable to perform all testing	20	2	0.4	Mid	Internal	Mitigate
D	4	Test reports do not identify any vulnerabilities	15	4	0.6	Far	Internal	Watch
E	5	Industry stakeholders attempt to suppress or invalidate results	20	5	1	Far	Internal	Watch

8.0 Investment Benefit/Program Impact

- DHS has a mandate to improve cybersecurity across all sectors: PPD-21, QHSR
- Short and long term National Security Impact
- Impact and establish policy leading to long term aviation cyber defense posture
- Significantly improve overall cybersecurity resiliency, addressing gaps, data collection, and mitigation to meet emerging aviation cyber vulnerabilities
- Allow for rapid prototyping and testing new technologies
- Provide vendors guidance to develop and integrate desired features to their solutions

BACKUP

Page 098 of 117

Withheld pursuant to exemption

(b)(7)(E);(b)(7)(F)

of the Freedom of Information and Privacy Act

ACI Research and Development FY17 and beyond Flight Plan

21 March 2017

Dr. Robert (Rob) Hickey
Program Manager
Cyber Security Division

Introduction

- Aircraft Cyber Evaluation (ACE) completed in Sep 2016
- FY17
- FY18 and beyond

Economic Reality

Most current data indicates U.S. civil aviation accounted for:

- $1.6 trillion in total annual economic activity
- Supported 10.6 million jobs – 8.5% of all U.S.
- Contributed 5.1% to the U.S. GDP
- Civil aircraft manufacturing top net U.S. export; $60 billion positive trade balance

Most current data indicates U.S. general aviation accounted for:

- $150 billion annual economic contribution
- 1.2 million jobs

Globally, each day more than $18.6 billion of goods travel by air; one-third of all trade by value

- $2.4 trillion global economic impact; 58 million jobs globally

5.1% of U.S. GDP…12 Million U.S. Jobs and 58 Million Jobs Globally!

Slide courtesy of the NAI2O

A Day in the Aviation Domain

- **Domestically**
  - 23,911 commercial flights
  - 2.3 million passengers
  - 7,000 planes in the sky at any given moment
  - Generating $2.6 billion in economic activity
- **Military (*based on 3-month average*)**
  - Personnel – 1,769
  - Cargo – 819 tons
  - Off-loads – 87
  - Planned sorties – 1,198
    - Airlift: 222; Refueling: 60; Training: 263; Other: 54

Internationally

- 93,000 commercial flights
- 8.4 million passengers
- 13,000 planes in the sky at any given moment
- Generating $7.4 billion in economic activity
- 59,466 commercial airports and civ/mil airports/airfields

Slide courtesy of the NAI2O

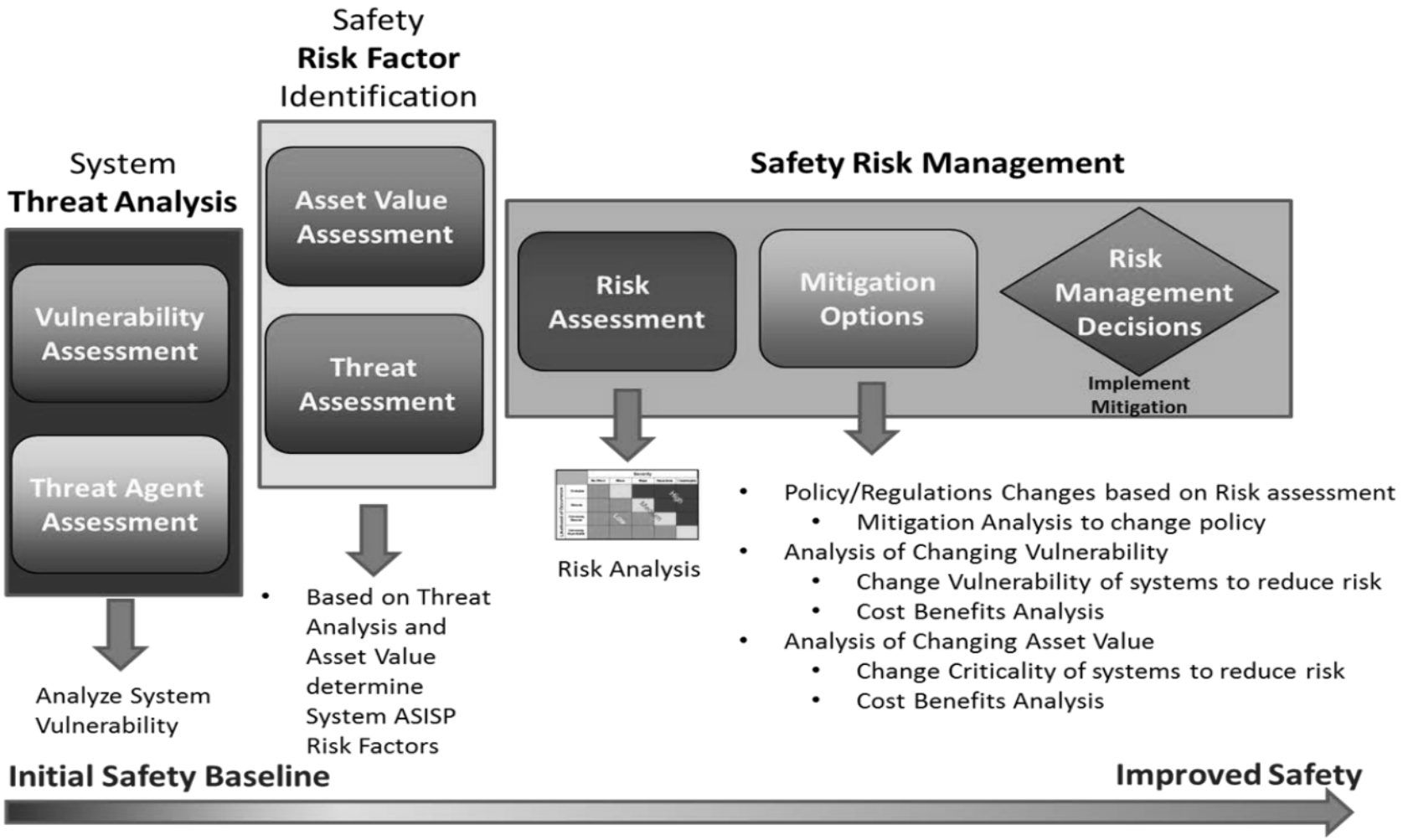
Federal Aviation Administration William J. Hughes Technical Center, Atlantic City, NJ

Aircraft Systems Information Security Protection (ASISP) Research Need

- Research is needed to assess:
  - ASISP **vulnerabilities**, **risks**, and
  - Explore possible **mitigations**

- Methodology is required to systematically guide the potential development of:
  - ASISP regulation, policy, and guidance for the certification and continued airworthiness of aircraft
- DHA S&T through the ACI Research and Development will contribute to filling that need

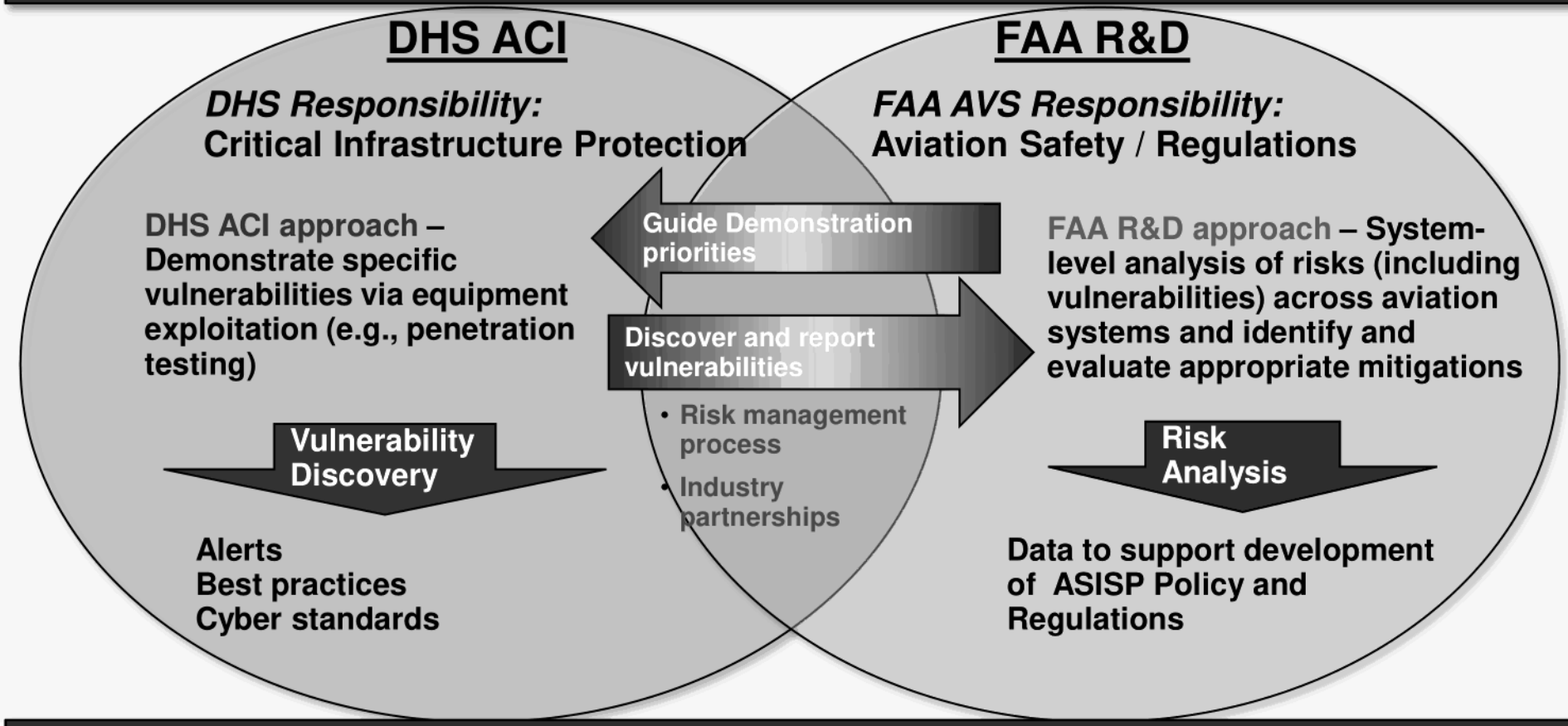
ASISP Safety Risk Assessment Research Framework



ASISP Research Activities

(**Aircraft Systems** Information Security/Protection - ASISP)

FAA ASISP & DHS ACI R&D Partnership for Aircraft Cyber Risk Mitigation



Synergistic multiagency collaboration to address aviation cyber threats

FY17 Electrical System

Potential SRA Subject	ACI R&D - Electrical Systems	Organization Name: What you are doing in this area that you would be willing to share.
Heads-Up Display (HUD)	Heads-Up Display (HUD)	
Engine Indicating and Crew-Alerting System (EICAS)	Engine Indicating and Crew-Alerting System (EICAS)	
Electronic Centralized Aircraft Monitor (ECAM)	Electronic Centralized Aircraft Monitor (ECAM)	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Cabin Printer	
Automatic Dependent Surveillance Contract (ADS-C)	(Multifunction) Control Display Unit ((M)CDU)	
Cabin Printer	Electronic Flight Bag (EFB)	
(Multifunction) Control Display Unit ((M)CDU)	Multifunction Display (MFD)	
Mode-S Transponders	Primary Flight Display (PFD)	
Electronic Flight Bag (EFB)	Autopilot (A/P)	
Multifunction Display (MFD)	Cabin Pressure Control System (PCS)	
ADS-B In	Engines	
Primary Flight Display (PFD)	Full Authority Digital Engine Control (FADEC)	
Flight Control Servos	Autothrottle/Thrust Management Unit (TMU/TMC)	
Flight Control System (FCS)	Flight Management System (FMS)	
Autopilot (A/P)	Traffic and Collision Avoidance System (TCAS)	
Instrument Landing System (ILS)	Air Data Computer (ADC)	
Marking Beacon Receiver	Communications Management Unit (CMU)	
Microwave Landing System (MLS)	Fuel Quantity Management System	
Attitude Heading and Reference System (AHRS)	Weather RADAR	
Cabin Pressure Control System (PCS)		
Engines		
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Lightning Detector		
Clock		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

FY17 FMS

Potential SRA Subject	ACI R&D - FMS	Organization Name: What you are doing in this area that you would be willing to share.
Heads-Up Display (HUD)	Engine Indicating and Crew-Alerting System (EICAS)	
Engine Indicating and Crew-Alerting System (EICAS)	Electronic Centralized Aircraft Monitor (ECAM)	
Electronic Centralized Aircraft Monitor (ECAM)	Automatic-Dependent Surveillance Broadcast (ADS-B) Out	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Automatic Dependent Surveillance Contract (ADS-C)	
Automatic Dependent Surveillance Contract (ADS-C)	Cabin Printer	
Cabin Printer	(Multifunction) Control Display Unit ((M)CDU)	
(Multifunction) Control Display Unit ((M)CDU)	Multifunction Display (MFD)	
Mode-S Transponders	ADS-B In	
Electronic Flight Bag (EFB)	Primary Flight Display (PFD)	
Multifunction Display (MFD)	Autopilot (A/P)	
ADS-B In	Instrument Landing System (ILS)	
Primary Flight Display (PFD)	Autothrottle/Thrust Management Unit (TMU/TMC)	
Flight Control Servos	Flight Management System (FMS)	
Flight Control System (FCS)	Aircraft Personality Module (APM)	
Autopilot (A/P)	Global Positioning System (GPS)	
Instrument Landing System (ILS)	Inertial Reference System (IRS)	
Marking Beacon Receiver	Other nav sources (VOR/DME, Automatic Direction Finder)	
Microwave Landing System (MLS)	FMS Data Loader	
Attitude Heading and Reference System (AHRS)	Ethernet Switches (for Integrated Modular Avionics)	
Cabin Pressure Control System (PCS)	Data Transfer Unit	
Engines	Voice and data COMs, e.g. VHF, HF, SATCOM	
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Lightning Detector		
Clock		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

FY17 FADEC

Potential SRA Subject	ACI R&D - FADEC	Organization Name:
Heads-Up Display (HUD)	Engines	What you are doing in this area that you would be willing to share.
Engine Indicating and Crew-Alerting System (EICAS)	Full Authority Digital Engine Control (FADEC)	
Electronic Centralized Aircraft Monitor (ECAM)	Air Data Computer (ADC)	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Central Maintenance Computer	
Automatic Dependent Surveillance Contract (ADS-C)	Remote Data Concentrator	
Cabin Printer		
(Multifunction) Control Display Unit ((M)CDU)		
Mode-S Transponders		
Electronic Flight Bag (EFB)		
Multifunction Display (MFD)		
ADS-B In		
Primary Flight Display (PFD)		
Flight Control Servos		
Flight Control System (FCS)		
Autopilot (A/P)		
Instrument Landing System (ILS)		
Marking Beacon Receiver		
Microwave Landing System (MLS)		
Attitude Heading and Reference System (AHRS)		
Cabin Pressure Control System (PCS)		
Engines		
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

As Funding becomes available: Telemetry System

Potential SRA Subject	ACI R&D - Telemetry Systems	Organization Name:
Heads-Up Display (HUD)	Automatic-Dependent Surveillance Broadcast (ADS-B) Out	What you are doing in this area that you would be willing to share.
Engine Indicating and Crew-Alerting System (EICAS)	Automatic Dependent Surveillance Contract (ADS-C)	
Electronic Centralized Aircraft Monitor (ECAM)	Mode-S Transponders	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Instrument Landing System (ILS)	
Automatic Dependent Surveillance Contract (ADS-C)	Marking Beacon Receiver	
Cabin Printer	Microwave Landing System (MLS)	
(Multifunction) Control Display Unit ((M)CDU)	Radar Altimeter	
Mode-S Transponders	Inertial Reference System (IRS)	
Electronic Flight Bag (EFB)	Other nav sources (VOR/DME, Automatic Direction Finder)	
Multifunction Display (MFD)	Attitude Heading and Reference System (AHRS)	
ADS-B In		
Primary Flight Display (PFD)		
Flight Control Servos		
Flight Control System (FCS)		
Autopilot (A/P)		
Instrument Landing System (ILS)		
Marking Beacon Receiver		
Microwave Landing System (MLS)		
Attitude Heading and Reference System (AHRS)		
Cabin Pressure Control System (PCS)		
Engines		
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

As Funding becomes available: Environmental System

Potential SRA Subject	ACI R&D - Environment/Life Support	Organization Name:
Heads-Up Display (HUD)	Electronic Flight Bag (EFB)	What you are doing in this area that you would be willing to share.
Engine Indicating and Crew-Alerting System (EICAS)	Heads-Up Display (HUD)	
Electronic Centralized Aircraft Monitor (ECAM)	Cabin Pressure Control System (PCS)	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Voice and data COMs, e.g. VHF, HF, SATCOM	
Automatic Dependent Surveillance Contract (ADS-C)	In-flight entertainment system	
Cabin Printer	Cabin Printer	
(Multifunction) Control Display Unit ((M)CDU)	Airline Operations Center (AOC) Development Tool	
Mode-S Transponders		
Electronic Flight Bag (EFB)		
Multifunction Display (MFD)		
ADS-B In		
Primary Flight Display (PFD)		
Flight Control Servos		
Flight Control System (FCS)		
Autopilot (A/P)		
Instrument Landing System (ILS)		
Marking Beacon Receiver		
Microwave Landing System (MLS)		
Attitude Heading and Reference System (AHRS)		
Cabin Pressure Control System (PCS)		
Engines		
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

As Funding becomes available: Engines

Potential SRA Subject	ACI R&D - Engines	Organization Name:
Heads-Up Display (HUD)	Engine Indicating and Crew-Alerting System (EICAS)	What you are doing in this area that you would be willing to share.
Engine Indicating and Crew-Alerting System (EICAS)	Electronic Centralized Aircraft Monitor (ECAM)	
Electronic Centralized Aircraft Monitor (ECAM)	Autopilot (A/P)	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Engines	
Automatic Dependent Surveillance Contract (ADS-C)	Full Authority Digital Engine Control (FADEC)	
Cabin Printer	Autothrottle/Thrust Management Unit (TMU/TMC)	
(Multifunction) Control Display Unit ((M)CDU)	Air Data Computer (ADC)	
Mode-S Transponders	Central Maintenance Computer	
Electronic Flight Bag (EFB)		
Multifunction Display (MFD)		
ADS-B In		
Primary Flight Display (PFD)		
Flight Control Servos		
Flight Control System (FCS)		
Autopilot (A/P)		
Instrument Landing System (ILS)		
Marking Beacon Receiver		
Microwave Landing System (MLS)		
Attitude Heading and Reference System (AHRS)		
Cabin Pressure Control System (PCS)		
Engines		
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

As Funding becomes available: Autopilot System

Potential SRA Subject	ACI R&D - Autopilot/Landings Systems	Organization Name:
Heads-Up Display (HUD)	Engine Indicating and Crew-Alerting System (EICAS)	What you are doing in this area that you would be willing to share.
Engine Indicating and Crew-Alerting System (EICAS)	Electronic Centralized Aircraft Monitor (ECAM)	
Electronic Centralized Aircraft Monitor (ECAM)	Automatic-Dependent Surveillance Broadcast (ADS-B) Out	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out	Automatic Dependent Surveillance Contract (ADS-C)	
Automatic Dependent Surveillance Contract (ADS-C)	(Multifunction) Control Display Unit ((M)CDU)	
Cabin Printer	Mode-S Transponders	
(Multifunction) Control Display Unit ((M)CDU)	Multifunction Display (MFD)	
Mode-S Transponders	ADS-B In	
Electronic Flight Bag (EFB)	Primary Flight Display (PFD)	
Multifunction Display (MFD)	Flight Control Servos	
ADS-B In	Flight Control System (FCS)	
Primary Flight Display (PFD)	Autopilot (A/P)	
Flight Control Servos	Autothrottle/Thrust Management Unit (TMU/TMC)	
Flight Control System (FCS)	Flight Management System (FMS)	
Autopilot (A/P)	Traffic and Collision Avoidance System (TCAS)	
Instrument Landing System (ILS)	Air Data Computer (ADC)	
Marking Beacon Receiver	Voice and data COMs, e.g. VHF, HF, SATCOM	
Microwave Landing System (MLS)	Aircraft Personality Module (APM)	
Attitude Heading and Reference System (AHRS)	Terrain Avoidance and Warning System (TAWS)	
Cabin Pressure Control System (PCS)	Ground Proximity Warning System (GPWS)	
Engines	Radar Altimeter	
Full Authority Digital Engine Control (FADEC)	Global Positioning System (GPS)	
Autothrottle/Thrust Management Unit (TMU/TMC)	Inertial Reference System (IRS)	
Flight Management System (FMS)	Other nav sources (VOR/DME, Automatic Direction Finder)	
Traffic and Collision Avoidance System (TCAS)	Mode Control Panel (MCP)	
Air Data Computer (ADC)	Traffic Advisory System and Flight Information System Broadcast (FIS-B)	
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

As Funding becomes available: Fuel System

Potential SRA Subject	ACI R&D - Fuel Systems	Organization Name:
Heads-Up Display (HUD)	Engine Indicating and Crew-Alerting System (EICAS)	What you are doing in this area that you would be willing to share.
Engine Indicating and Crew-Alerting System (EICAS)	Electronic Centralized Aircraft Monitor (ECAM)	
Electronic Centralized Aircraft Monitor (ECAM)	Fuel Quantity Management System	
Automatic-Dependent Surveillance Broadcast (ADS-B) Out		
Automatic Dependent Surveillance Contract (ADS-C)		
Cabin Printer		
(Multifunction) Control Display Unit ((M)CDU)		
Mode-S Transponders		
Electronic Flight Bag (EFB)		
Multifunction Display (MFD)		
ADS-B In		
Primary Flight Display (PFD)		
Flight Control Servos		
Flight Control System (FCS)		
Autopilot (A/P)		
Instrument Landing System (ILS)		
Marking Beacon Receiver		
Microwave Landing System (MLS)		
Attitude Heading and Reference System (AHRS)		
Cabin Pressure Control System (PCS)		
Engines		
Full Authority Digital Engine Control (FADEC)		
Autothrottle/Thrust Management Unit (TMU/TMC)		
Flight Management System (FMS)		
Traffic and Collision Avoidance System (TCAS)		
Air Data Computer (ADC)		
Communications Management Unit (CMU)		
Fuel Quantity Management System		
Weather RADAR		
Voice and data COMs, e.g. VHF, HF, SATCOM		
Aircraft Personality Module (APM)		
Terrain Avoidance and Warning System (TAWS)		
Ground Proximity Warning System (GPWS)		
Radar Altimeter		
Global Positioning System (GPS)		
Inertial Reference System (IRS)		
Other nav sources (VOR/DME, Automatic Direction Finder)		
Mode Control Panel (MCP)		
FMS Data Loader		
Central Maintenance Computer		
Data Transfer Unit		
In-flight entertainment system		
Traffic Advisory System and Flight Information System Broadcast (FIS-B)		
Airline Operations Center (AOC) Development Tool		
Remote Data Concentrator		
Ethernet Switches (for Integrated Modular Avionics)		

As Funding becomes available: Electronic Flight Bag

- Just added

Way Forward

- FY17
- As funds become available
- Synergistic effects of those willing to share results, finding, and suggested requirements

QUESTIONS

Some things are too important NOT to share.

Homeland Security

BACKUPS