FAA Cybersecurity R&D Plan

(Version 1.0)

July 2017

Cybersecurity R&D Plan Version Control History

Version Number	Date	Description of changes
1.0	7/11/2017	Established FAA Cybersecurity R&D Plan and Released Version 1.0

Executive Summary

In recent years, the FAA has been stepping up modernization efforts that involve shifting air traffic control from ground-based technology to satellites. Airplane systems are also becoming increasingly automated and more connected to computer systems. While modernization has resulted in greater efficiency for the aviation industry, it has also made the FAA and the industry vulnerable to cyber-attacks because of the increasingly connected aviation ecosystem. Cybersecurity has become an elevated risk that is among the most pressing issues impacting the aviation industry today. Today's cyber adversaries are more persistent, skilled, and technologically savvy than ever before. According to PricewaterhouseCoopers' 2015 Global Airline Chief Executive Officer (CEO) Survey, 85% of CEOs in the aviation industry view cybersecurity as a significant risk. In a report released by the U.S. Government Accountability Office in 2015, the agency warned that increasing interconnectedness in the aviation industry can potentially provide unauthorized remote access to aircraft avionics systems and FAA-owned National Airspace Systems (NAS) that are of critical importance to the economic and national security of the U.S. In other words, the aviation ecosystem is becoming more and more vulnerable because cyber-attacks no longer require a physical connection to the targeted system to effectively attack it. It is imperative for the FAA to have programs and policies in place that can constantly monitor and keep pace with advancing and evolving threat vectors.

Cybersecurity represents one of the biggest challenges facing the FAA, and this Cybersecurity Research and Development (R&D) plan identifies research required to prevent, detect, and react to cyber-attacks, and to safely secure FAA NAS and mission support infrastructure. Example areas include communication systems; network-based information systems; satellite-based navigation, positioning, and timing systems, including Global Positioning System (GPS)-based timing; information technology; mission system automation; surveillance; and weather systems.

Although no information security system is absolutely foolproof, the FAA requires a comprehensive R&D program that provides operational capabilities to systematically prevent and detect cybersecurity attacks and help stakeholders react in ways that contain damage. These R&D plans examine each of these problem areas and discuss actionable steps for the FAA to manage evolving risks. This plan focuses on building cybersecurity capabilities that support the FAA's cybersecurity goals outlined in the FAA Cybersecurity Strategy 2017–2022 document. They include:

- *Goal 1—Refine and maintain a cybersecurity governance structure to enhance cross-domain synergy.*
- *Goal 2—Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery.*
- *Goal 3—Enhance data-driven risk management decision capabilities.*
- *Goal 4—Build and maintain workforce capabilities for cybersecurity.*
- *Goal 5—Build and maintain relationships with external partners in government and industry to sustain and improve cybersecurity in the aviation domain.*

This R&D plan further supports FAA leadership's efforts to balance and prioritize cybersecurity activities, based on risk and mission needs, and transform the strategies into effective tactical actions. Some of the requirements identified in this plan are still in the planning stages and will be initiated in the out-years pending appropriated funds. Others are funded and ongoing.

This R&D plan supports the *Cybersecurity Standards for Aircraft to Improve Resilience Act of 2016*, or the Cyber AIR Act (S.2764 – 114th Congress), and the *May 2017* Presidential *Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

Table of Contents

1.0 Introduction

The FAA manages and operates the nation's air transportation critical infrastructure. To achieve its mission of providing the safest, most efficient aerospace system in the world, the FAA is dependent on information systems. The FAA operates information systems in three domains:

1. National Airspace System (NAS) Domain—consists of more than a hundred systems and an ever-growing network infrastructure. The networking infrastructure is dedicated to the NAS operations and segregated from non-NAS infrastructures. The NAS provides the following five major FAA mission-critical services that directly support air travel: automation, communications, navigation, surveillance, and weather.
2. Mission Support Domain—provides common infrastructure of interconnected general support systems and services for the operation of administrative functions, such as messaging services, financial and grants applications, *non-mission-critical NAS applications, airman and aircraft certification and regulatory services, commercial space applications,* and airport services, and hosts the FAA's two Internet Access Points. The mission support domain is operated by FAA Information and Technology (AIT) Service organization, the newly formed Information Technology (IT) shared services organization. AIT provides oversight, management and control over all IT programs and projects, daily operations and maintenance activities, the IT infrastructure and regionalized operations including the FAA's data centers, telecommunications and IT management functions.[1]
3. Research and Development (R&D) Domain: with a separate security perimeter that provides an environment for research activities and for development programs and industry partners to share information. The R&D domain provides a limited emulation of the FAA systems environment and provides a safe conduit to share information for R&D purposes.

Communication and data flows between these three domains are controlled through the use of gateways to assure that cross-domain traffic is monitored and managed.

Cybersecurity is a key mission enabler for the FAA. The need to protect the critical infrastructure of the national airspace and participate in the protection of the aviation sector as a whole from cyber threats, vulnerabilities, and attacks is clear. To meet this challenge, the FAA is taking a collaborative and holistic enterprise-wide approach to cybersecurity strategy research that ensures an informed and coordinated method to cyber risk management while maintaining the flexibility for domain-specific tactics towards implementation and execution.

As the modernization of aircraft and air traffic management becomes more reliant on networks and communications in an effort to become more efficient, the fundamental requirement for

[1] This version of the plan does not contain any identified R&D requirements that address the agency's administrative functions.

safety must be maintained. The new technologies implemented to improve efficiency have their own intrinsic vulnerabilities that impact the security of FAA systems and must be balanced with maintaining aerospace efficiency. The FAA has prioritized the security of these systems, whether existing NAS or the development of new systems through NextGen. Securing these existing and evolving technologies and systems is critical in fulfilling the FAA's mission of safety and efficiency.

1.1 Public Law 114-190/Section 2111

As mandated by Congress in the FAA Extension, Safety and Security Act of 2016, the FAA is required to "*facilitate and support the development of a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the national airspace system, civil aviation, and agency information systems using a total systems approach that takes into consideration the interactions and interdependence of different components of aircraft systems and the national airspace system.*"

In accordance with Section 2111(e) of the Act: *…, the Administrator, in consultation with other agencies as appropriate, shall establish a cybersecurity research and development plan for the national airspace system, including -*

(1) Any proposal for research and development cooperation with international partners;
(2) An evaluation and determination of research and development needs to determine any cybersecurity risks of cabin communications and cabin information technology systems on board in the passenger domain; and
(3) Objectives, proposed tasks, milestones, and a 5-year budgetary profile.

This 5-year Cybersecurity R&D Plan, to be updated annually, is pursuant to Section 2111 (e). The intent of this plan is to frame the next 5-year research portfolio (i.e., all ongoing and prospective R&D activities relative to the goals and objectives specified in the Cybersecurity Strategy 2017–2022).

1.2 Governance

On May 11, 2017, the President issued the new Executive Order "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which reinforces the essential role cybersecurity plays in protecting the nation's critical infrastructure. It establishes responsibilities for Departments and Agencies, including the FAA, in a public/private partnership to secure the nation's critical infrastructure from cyber threats. Along with EO 13636, Presidential Policy Directive (PPD) 21 "Critical Infrastructure Security and Resilience" directs departments and agencies, including the FAA, to develop situational awareness of the functional health of infrastructure from a cyber-perspective. The FAA has the responsibility to secure interoperable systems and capabilities as a partner in the aviation enterprise.

Each requirement identified in this plan has been mapped to a specific cybersecurity research area. In addition, the requirements have defined output(s) and intended outcome(s). Where

applicable, the research will reference the latest version of the National Institute of Standards and Technology (NIST) of security guidance for information systems.

The requirements contained within this plan have been vetted/validated through the following two FAA groups, the Cybersecurity Steering Committee (CSC) and the Research, Engineering, and Development Advisory Group (REDAC).

2.0 Research Portfolio

2.1 R&D Plan Framework

The requirements contained in this Cybersecurity R&D plan address needs in all three domains described in Section 1 and align to the five FAA goals defined in the Cybersecurity Strategic Plan (2017-2022). Three of the five strategic goals most relevant to Research & Development are highlighted in italics:

(1) Goal 1-Refine and maintain a cybersecurity governance structure to enhance cross-domain synergy.
(2) Goal 2—Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery.
(3) Goal 3—Enhance data-driven risk management decision capabilities.
(4) Goal 4—Build and maintain workforce capabilities for cybersecurity.
(5) Goal 5—Build and maintain relationships with external partners in government and industry.

In addition, Section 7, Technical Collaboration, of this plan aligns with FAA Goal 5. The requirements that address FAA goals were further categorized by research areas and are addressed in Sections 3, 4, 5, and 6 of the plan. Figure 1 illustrates the mapping of the FAA goals to the various research areas identified in this R&D plan.

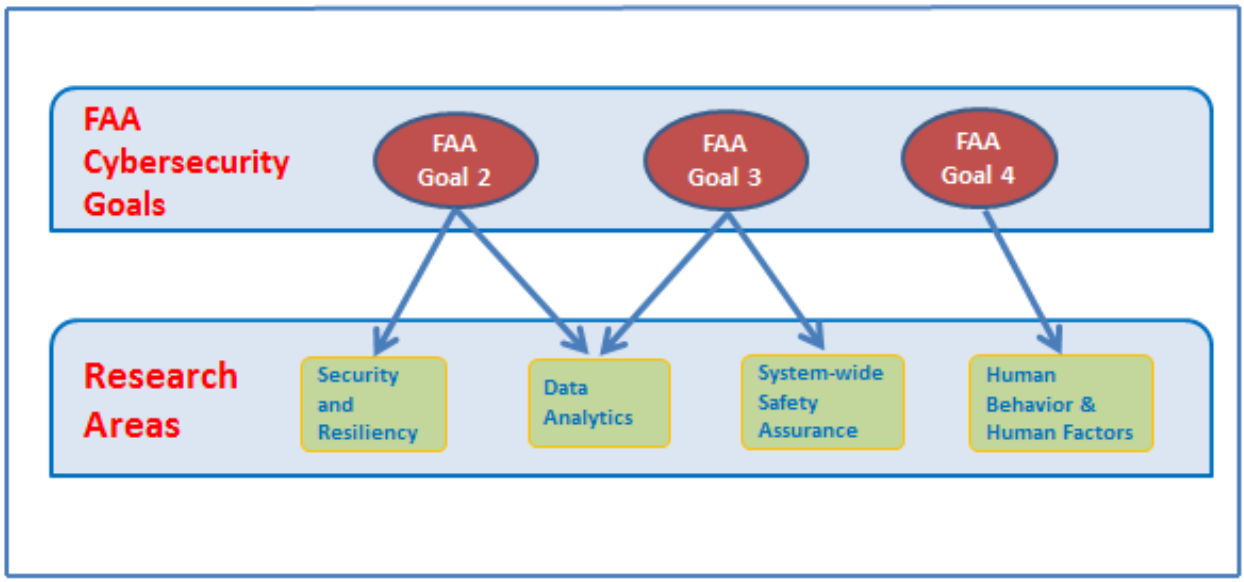

Figure 1: Cybersecurity R&D Plan-Mapping of FAA Cybersecurity Goals to Research Areas

2.2 Research Areas

The research requirements presented in this plan are aligned with the following research areas:

- **Security and Resiliency**—Develop methods to enhance the FAA's ability to prevent, detect, and respond to cyber-attacks.

- **Data Analytics**—Develop analytical capabilities for aggregating and correlating current data with the intent of understanding, predicting, and responding to cyber-attacks.
- **Human Behavior/Human Factors**—Develop and validate human-in-the-loop policies, training, and procedures to detect and respond to cyber-attacks.
- **System Wide Safety Assurance**—Develop real time, continuous, safety analysis and assurance tools and capabilities to prevent/mitigate the impact of cyber-attacks.

The breadth and depth of research requirements covering these research areas will provide the FAA with enhanced operational capabilities to systematically prevent and detect cybersecurity attacks and help various stakeholders react in myriad ways that contain damage.

2.3 Proposed Research

Each research requirement identified in this plan contains a brief overview, a list of proposed tasks, critical milestones, anticipated outcome of the research, and a 5-year budgetary profile. Regarding the budget data, FY18 is the amount that has been requested through the President's budget submission. The FY19 represents the submitted amount to the Office of Secretary of Transportation. All other funding information shown should be considered "estimates."

In situations in which the research topic has not been fully defined, it is identified as a research need. These needs are listed because they are perceived gaps in one of the research areas. In future updates to this plan, it is anticipated that these needs will evolve into clearly defined requirements.

3.0 Research Area—Security and Resiliency

Develop methods to enhance FAA's ability to prevent, detect, and respond to cyber-attacks.

The FAA has taken on measures to protect its networks and systems, including: boundary protection; authentication and access controls; cyber operations and event monitoring; threat coordination with actionable threat information; and promotion of cybersecurity information sharing. These protective measures are effective to protect the networks and systems "as-is" with identified attacks against known vulnerabilities.

The challenges still remain on protecting and defending the FAA systems from both internal and external threats of rapid advances and sophistication of cyber-attacks, ever-evolving systems with new connectivity, and increased interdependencies of the FAA internal networks and external stakeholder systems of the ever-expanding aviation ecosystem

Radio frequency (RF) "wireless" data messages are used by aviation information systems, mission systems, and supporting critical infrastructure. These systems are vulnerable to cyber-data spoofing. Examples of these system dependencies include RF satellite and terrestrial data communications and the numerous systems that are dependent upon the use of GPS time. The radio-frequency threats include new GPS cyber-data spoofing threats. These threats will be assessed and addressed as appropriate in the annual update of this plan.

3.1 Aircraft Systems Information Security Protection (ASISP) Requirement

3.1.1 Description

Aircraft manufacturers and modifiers are installing systems with network-centric architectures that allow increased wired and wireless connectivity to aircraft systems within an aircraft and to networks external to the aircraft. These network-centric architectures may have aircraft systems information-security-protection vulnerabilities that could negatively impact aircraft airworthiness if exploited. Unauthorized access to aircraft systems and networks could result in the malicious use of networks and loss or corruption of data (e.g., software applications, databases, and configuration files) brought about by software worms, viruses, or other malicious entities. Research is needed to identify aircraft systems information-security-protection vulnerabilities, risks, and mitigations to guide the potential development of regulation, policy, and guidance for their certification and continued airworthiness. The purpose of this research is to assess/analyze wired and wireless connectivity to aircraft systems to identify information-security-protection vulnerabilities and risks that could adversely affect the safety of an aircraft by compromising the fail-safe mechanisms intended to mitigate the effects of aircraft and systems equipment and component failures. The research should also recommend what measures—including but not limited to architectural, design, and process assurance measures, and flight crew and

maintenance crew actions—would be effective in mitigating these aircraft systems information-security-protection-related vulnerabilities and risks.

3.1.2 Initiatives/Tasks

These research tasks include identifying, assessing, and providing recommendations for mitigation of security vulnerabilities in aircraft net-centric architectures and internal/external wired and wireless interfaces that could affect aircraft safety. The research will guide potential aircraft systems information security-protection-related rulemaking, policy development, and guidance for best practices. The specific tasks are to:

- Define, identify, and assess vulnerabilities and risks associated with wired and wireless aircraft systems interfaces that could affect aircraft safety.
- Identify and recommend mitigations for the vulnerabilities and risks found from Task 1.
- Identify and recommend strategies associated with tasks 1 and 2 for aircraft certification, maintenance, and continued operational safety.

An objective of the Aircraft Systems and Information Security Program (ASISP) research initiative is to establish a safety risk assessment (SRA) methodology, based on the ASISP research framework shown in figure 2, and to implement the methodology on a selected set of SRA subjects.

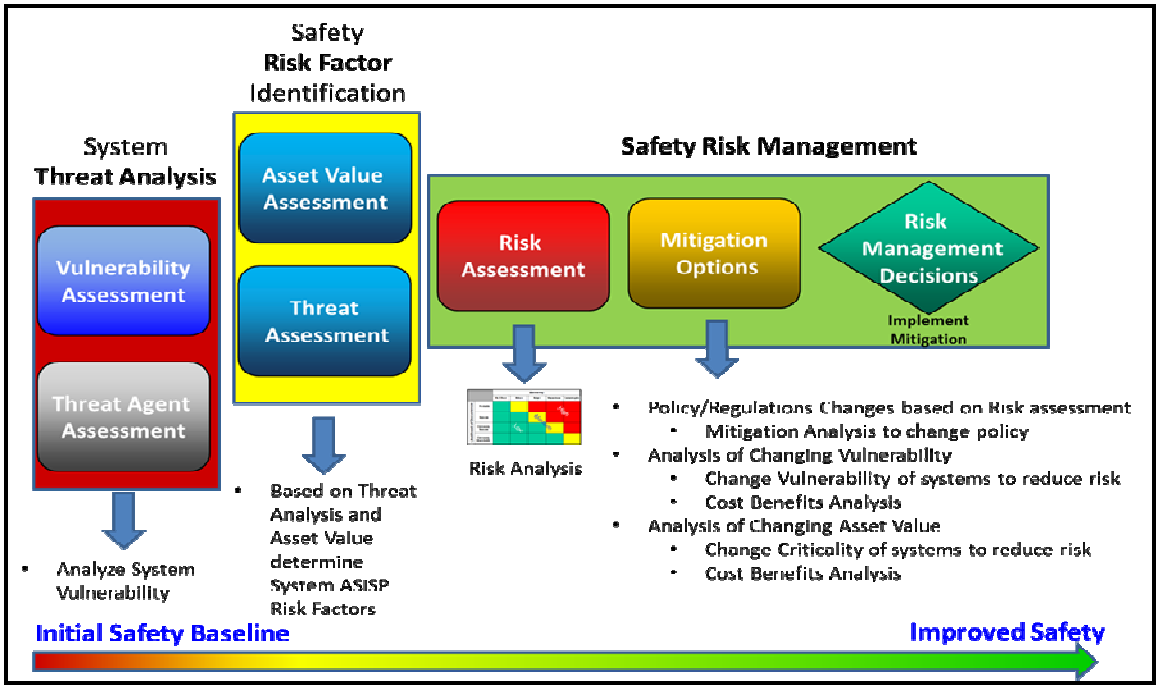

Figure 2: ASISP Research Framework—Threat and Risk Assessment

3.1.3 Critical Milestones/Outputs

- FY17—Initial SRA of Aircraft Addressing and Reporting System

- FY18—Safety risk methodology for analysis of security threats to aircraft safety in an airborne network environment
- FY19—Initial set of ASISP risk-mitigation processes within the SRA framework.
- FY20 – ASISP methodology/SRA and risk mitigation processes.
- FY21 – Comprehensive ASISP safety risk management process and guidelines (for use in the development of new FAA regulations, policy, standards, guidance, and training).

3.1.4 Outcome

The research outputs will provide insights into information-security-protection vulnerabilities of, and risks to, aircraft systems, components, networks, and interfaces that would provide a basis for developing rulemaking, policy, guidance, standards, training, and tools for security.

3.1.5 Funding Profile

	Year 1 2018	**Year 2 2019**	**Year 3 2020**	**Year 4 2021**	**Year 5 2022**
Funding	$2,000K	$2,100K	$2,600K	$2,200K	$2,000K

Status: A multi-year, ongoing R,E&D-funded requirement

3.2 Cybersecurity Risks of Cabin Communications and Cabin IT Systems—Requirement

3.2.1 Description

With the advent of integrated modular avionics architectures in all modern aircrafts, airplane systems are increasingly automated and more connected to computer systems. Whereas modernization has resulted in greater efficiency for the aviation industry, it has also made the FAA and the industry vulnerable to cyber-attacks because of the increasingly connected aviation ecosystem. This problem is further compounded by the proliferation in the use of personnel electronic devices, and cyber-attacks no longer require a physical connection to the targeted system to effectively attack it. Section 2111e within the enacted Public Law 114-190 states that the FAA administrator shall [conduct] "… an evaluation and determination of research and development needs to determine any ***cybersecurity risks of cabin communications and cabin information technology systems on board in the passenger domain."***

This research, which addresses the Congressional mandate, will leverage related research into the development of an SRA methodology for the Aircraft Systems Information Security Program. The initial focus will be on the identification of aircraft system architectures that are likely to include cabin communication and information systems and configurations that are susceptible to

cybersecurity attacks. SRAs of the relevant systems will be conducted, resulting in SRA reports that document and quantify the risks, and any discovered vulnerabilities. In addition to analytical assessment, this research plan will use a system integration laboratory that appropriates representative aircraft equipment configurations necessary for conducting adversarial penetration testing and reverse engineering to identify vulnerabilities that could lead to safety risk to the aircraft. The analytical risk assessments would establish risks so informed mitigation decisions could be made. The adversarial testing provides validation of analytical findings and potential discovery of vulnerabilities and risks not uncovered by analytical means alone.

3.2.2 Initiatives/Tasks

1. Identify the aircraft system architectures and cabin communication and information systems that need to be studied.
2. Determine and assess the cybersecurity risks to aircraft safety.
3. Conduct adversarial exploitation testing of cabin communication and cabin information systems in a lab environment to discover vulnerabilities and augment the risk assessment conducted in Task #2.

3.2.3 Critical Milestones/Outputs

- FY19—Technical report that identifies the scope of aircraft architectures, cabin communication, and information that needs to be studied
- FY20—Initial risk assessments of selected systems
- FY21—Technical data generated from adversarial exploitation testing in a lab environment
- FY22—Technical report that includes the identification and assessment of any safety risks
- FY22—Technical report that includes the identification of discovered vulnerabilities

3.2.4 Outcome

The research outputs will provide insights into information-security-protection vulnerabilities of, and risks to, cabin communication and IT systems, associated components, networks, and interfaces that would provide a basis for developing rulemaking, policy, guidance, standards, training, and tools for security.

3.2.5 Funding Profile

	Year 1 2018	Year 2 2019	Year 3 2020	Year 4 2021	Year 5 2022
Funding	$0	$2,000K	$2,000K	$2,000K	$2,000K

Status: Approved multi-year R,E&D requirement planned to be initiated in FY19

3.3 Unmanned Aircraft Systems Networked Command and Control Link Systems Security Protection - Requirement

Unmanned aircraft systems (UAS) present an especially difficult challenge to safety because the pilot is not physically located in the aircraft. For manned aircraft, the pilot always has the ability to manually take control of the aircraft should the pilot have reason to believe any system in the aircraft is not performing. This is not the case for all unmanned aircraft systems. The pilot must rely on a multitude of systems all working securely to maintain control of the aircraft.

3.3.1 Description

The Radio Technical Commission for Aeronautics (RTCA) SC-228 (Minimum Operational Performance Standards [MOPS)]) and the FAA have identified security risks associated with the operation of UAS control and non-payload communications (CNPC) link systems and networks supporting the operation of large and small UAS in the NAS. CNPC links require secure communication between unmanned aircraft, the control station, and the networked system. Security for the command and control (C2) data link and its network system is critical and must be ensured for UAS C2 communications and mission viability.

This research directly supports the development of FAA TSOs and Advisory Circulars (ACs) for UAS new unique and safety critical C2 beyond line of sight (BLOS) networked terrestrial and satellite Link Systems security control with high levels of sophistication, publication of operational guidance materials, and Path Finder certification activities. A representation of the UAS notional architecture is shown in figure 3.

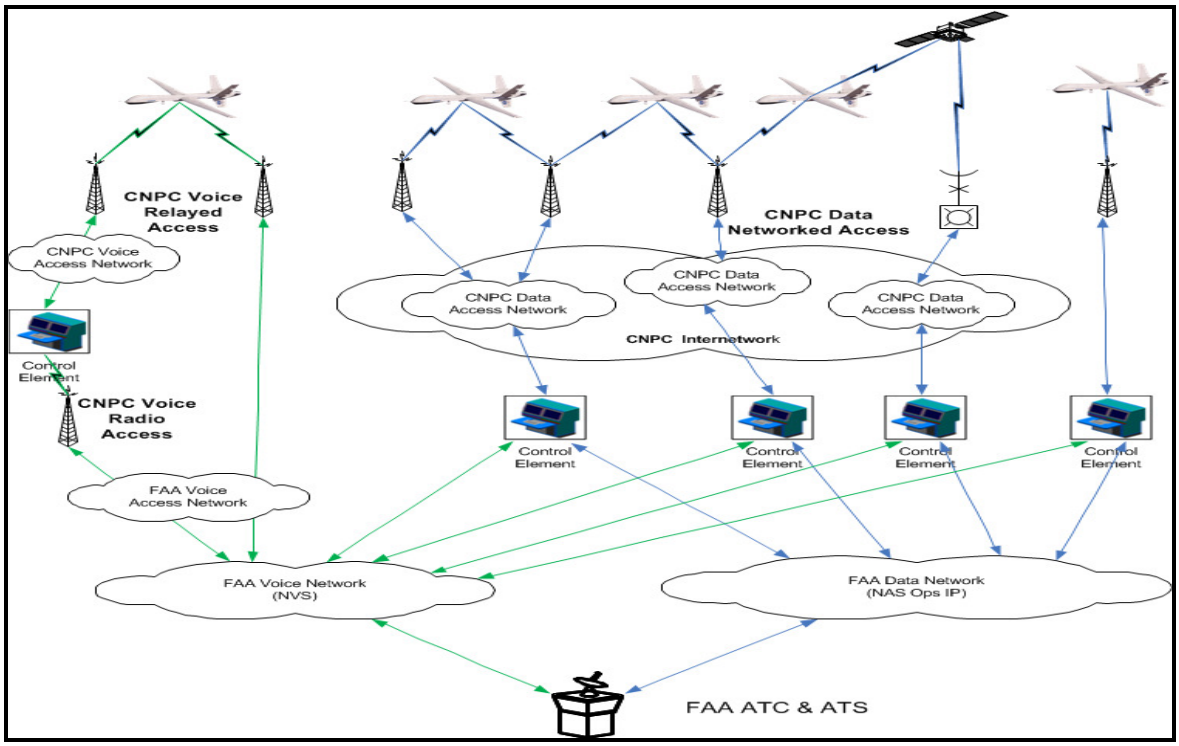

Figure 3: UAS Notional Architecture

This research requirement supports the design of robust C2 links that can achieve sufficient link performance and availability while providing necessary security to ensure the CPNC radio link in a networked configuration will in turn support the safe integration of this new technology into the NAS.

Research will address the following UAS C2 link requirements:

- Allow cryptographic algorithms and strengths
- Provide confidentiality, integrity, and authentication controls for end-to-end link security
- Provide data origin authentication (per message/frame) and strength
- Provide flexibility for implementation by developers

3.3.2 Initiatives/Tasks

This multi-year research requires testing to assess and efficiently and effectively mitigate against security threats of network terrestrial and SatCom C2 data-link systems with a high level of sophistication.

- Evaluate the RTCA SC-228 on communication security controls for C2 terrestrial network systems and address end-to-end communication security and air-to-ground control plane security.

- Conduct testing to demonstrate efficient and effective communication security controls for C2 terrestrial networked system.
- Evaluate the SC-228 MOPS on communication security controls for C2 SatCom network systems, and conduct testing to demonstrate efficient and effective communication security controls for C2 terrestrial networked system.
- Recommend requirements and guidance on minimal protocol-related security framework for implementing communication security controls for protection of networks of terrestrial and SatCom C2 data link systems.

3.3.3 Critical Milestones/Outputs

- FY19: Detailed results of bench tests to assess and mitigate various types of security threats against networks of terrestrial and SatCom C2 data-link systems with a high level of sophistication
- FY21: Report providing guidance on implementing communication security controls for networked CNPC Link Systems Security Protection of networks of terrestrial and SatCom C2 data link

3.3.4 Outcome(s)

The results of this research will be used in the development of guidance material (i.e., ACs and TSOs for UAS C2 Link system addressing CNPC Link system security protection, support of FAA path finder certification activities, or publication of operational guidance materials) and other related activities.

3.3.5 Funding Profile

Resource Table

	Year 1 2018	**Year 2 2019**	**Year 3 2020**	**Year 4 2021**	**Year 5 2022**
Funding	$310K	$330K	$350K	$0K	$0K

Status: Approved multi-year R,E&D requirement planned to be initiated in FY18.

3.4 Information Security Protection Associated with UAS Integration into NAS—Research Need

UAS integration into the NAS is occurring at an alarming pace. One of the key integration challenges that various stakeholders associated with UAS must contend with is information security. Security efforts are currently underway regarding the C2 component of UAS. The RTCA SC-228 and the FAA have identified security risks associated with the operation of UAS CNPC link systems and networks supporting the operation of UAS in the NAS and mitigating controls to reduce the level of impact those risks pose to the systems. Research is currently underway that supports the development of the FAA's new TSO requirements and AC guidance for UAS new, unique, and safety-critical C2 BLOS networked terrestrial and satellite Link Systems security control with a high level of sophistication. The research supports the Path Finder certification activities. The outputs will provide technical data for publication of operational guidance materials.

In addition to addressing the UAS C2 link component, it is of critical importance for the FAA to address the security of the UAS to NAS communications. This research will focus on information security concerns associated with:

- UAS pilot to/from NAS—Data communications.
- UAS pilot to/from NAS—Voice communications.
- UAS flight plans.
- UAS departure clearances.

The research outputs will provide insights into information security protection vulnerabilities of, and risks associated with, integration of UAS into NAS components, networks, and interfaces that would provide a basis for developing rulemaking, policy, guidance, standards, training, and tools for enhanced security. The tasks, milestones, research outcomes, and resources required will be provided in a future update to the R&D plan.

3.5 Development of a Comprehensive UAS Centric Cybersecurity Risk Management Framework—Research Need

From a risk-based perspective, UAS cybersecurity is no different than any of the cybersecurity needs of the current and future NextGen NAS information providers, Navigation Communication and Surveillance (CNS) systems, and any system required to support safe risk-based decision making. This risk-based decision making, which is one of the four strategic pillars outlined by the FAA administrator, requires the development of a comprehensive UAS cybersecurity risk-management framework.

Unauthorized access to UAS and associated networks could result in the malicious use of networks and loss or corruption of data (e.g., software applications, databases, and configuration

files) brought about by software worms, viruses, or other malicious entities. Research is needed to identify UAS information-security-protection vulnerabilities, risks, and mitigations to guide the potential development of regulation, policy, and guidance for certification and continued airworthiness.

The research will recommend what measures, including but not limited to architectural, design, and process assurance measures, would be effective in mitigating the UAS information security protection related vulnerabilities and risks. The tasks, milestones, research outcomes, and resources required will be provided in a future update to the R&D plan.

4.0 Research Area—Data Analytics

Develop analytical capabilities for aggregating and correlating current data with the intent of understanding, predicting, and responding to cyber-attacks.

4.1 Flight Deck Data Exchange—Requirement

4.1.1 Description

The Flight Deck Data Exchange research initiative addresses the data exchange-format and performance requirements to enable enhanced data exchange between onboard avionics systems and ground systems to support Trajectory Based Operations (TBO). Recent advancements in flight-deck automation, such as electronic flight bags, aircraft interface devices, and the availability of new on-board data links have introduced an opportunity for flight operators to leverage these technologies in the collaborative decision-making process. There is ongoing work to evaluate the feasibility of using these technologies to enable operational functions, such as trajectory negotiation and downlink of aircraft-specific intent data to synchronize trajectories with ground automation with extensive work in improving the ground automation capabilities, but further research is required on the flight-deck automation-performance requirements.

This initiative will enable flight operators, Air Traffic Management (ATM) personnel, and their respective automation systems to improve operational efficiencies in the NAS by enabling the necessary data exchange required to establish a TBO NAS. This research leverages emerging technologies on the flight deck to exchange aircraft-specific data that will allow ground automation systems and air traffic controllers to have precise information on the future position and state of an aircraft, reducing the need for large separation requirements caused by uncertainties. This research and these emerging technologies will enable the flight operators to navigate around constraints that are specific to their individual operational needs and capabilities by allowing them to negotiate trajectory options that incorporate their aircraft-performance capabilities and operational priorities. These improvements will support the implementation of a TBO NAS that reduces the inefficiencies caused by the rigid navigation structures and the current limitations with controllers' ability to space and merge traffic in a performance-based navigation environment. This research will also address the security requirements to ensure safe and effective information exchange between aircraft and ground automation systems by evaluating and establishing recommendations for systems onboard aircraft.

4.1.2 Initiatives/Tasks

The research will evaluate the security requirements to enable safe data exchange between certified and non-certified systems, the performance standards required to enable operational information exchange, and the data-exchange protocols to enable seamless integration between airborne and ground systems. The agency will also seek to evaluate and address the security

requirements for information exchange and interaction between certified and non-certified avionics, and between airborne and ground automation systems, to maintain the integrity of systems that are safety critical to flight operations while enhancing data-exchange capabilities. Tasks include, but are not limited to:

- Developing a research plan for flight-deck data-exchange requirements
- Developing an initial technical and operational assessment report
- Developing initial concept, scenarios, and use cases
- Identifying flight-deck information-exchange architecture alternatives
- Initiating flight-deck data-exchange requirements research
- Validating concept, scenarios, and use cases
- Conducting ASISP response and recovery simulation of operational scenarios and use cases

4.1.3 Critical Milestones/Outputs

- FY20—Comprehensive research plan for flight-deck data-exchange requirements
- FY21—Fully developed prototype environment
- FY22—ASISP response and recovery simulations of scenarios and use cases
- FY22—Final draft report containing research findings on recommended flight-deck data-exchange requirements and performance standards

4.1.4 Outcome

With increased participation of a number of aircraft in the necessary data-exchange environment, it is envisioned that flight operators will be able to operate at their optimal performance envelopes while reducing the need for air traffic control (ATC) intervention and restrictions by enabling reduced and delegated separation management.

4.1.5 Funding Profile

	Year 1 2018	**Year 2 2019**	**Year 3 2020**	**Year 4 2021**	**Year 5 2022**
Funding	$0	$2,000K	$2,100K	$2,200K	$2,200K

Status: Approved R,E&D multi-year requirement that is planned to be initiated in FY19

4.2 NextGen-Information Security - Requirement

4.2.1 Description

The NAS continues to evolve with operational improvements through implementation of NextGen technologies to enhance safety with improved efficiency. These operational improvements, along with broad applications of new and advanced technologies in various areas by the NAS stakeholders and users, will allow increased digital connectivity with various networks and services of the FAA enterprise to receive services and related information.

The FAA Cybersecurity Roles and Responsibilities, N1370.47, as updated and approved by the FAA CSC, clearly defines the roles and responsibilities of FAA internal organizations to protect and defend the FAA enterprise, which comprises three domains: the NAS Domain, Mission Support, and R&D. Each of the domains provides distinct functions and services, which work together collectively to support the overall FAA mission of providing "*the safest, most efficient aerospace system in the world*." These systems have their own unique architectures, network connectivity, and system configurations with specific security goals and objectives. The FAA has established separate security perimeters for each of the domains and implemented various boundary protection technologies, advanced authentication tools, security policies, and internal controls to maintain and improve security postures of these domains.

Although these protections are effective to mitigate the risks of cyber-attacks with known vulnerabilities, the FAA is facing challenges of unknown attack vectors, newly discovered vulnerabilities (zero-day attacks), increased sophistication of adversaries, state-sponsored terrorism, etc. The rapidly evolving capabilities of the potential adversaries and decreasing costs of exploits necessitates some prudent exploration of advanced detection and defense capabilities that the FAA can use to analyze, evaluate, and respond in a timely manner. New mitigation solutions may be necessary as the FAA systematically implements new technologies to achieve NextGen goals and deliver safer and more efficient services to NAS stakeholders and users.

Research and evaluation are needed to investigate the effectiveness of cyber-protection techniques/methodologies in response to the challenges of the dynamic nature of cyber-threats.

4.2.2 Initiatives/Tasks

The purpose of this research is to help prevent disruptive cyber incidents that affect the ATC mission and improve resiliency in the event an incident does occur. This research supports the FAA's overall cybersecurity development by researching advanced tools, techniques, and processes that can be adapted for use in the NAS. The research also further supports EO 13636-Improving Critical Infrastructure Cybersecurity and the PPD-21 Critical Infrastructure Security and Resilience, which defines the transportation systems sector as one of the critical infrastructure sectors.

This research effort includes collaboration with other Government agencies, primarily the Department of Homeland Security (DHS), Science and Technology (S&T), and the U.S. Air Force Research Laboratory, to support the FAA cybersecurity needs. The specific tasks are to:

- Develop advanced big data analytics approaches to detect and respond to advanced persistent and insider threats.
- Investigate the feasibilities of applying impact-assessment and risk-analysis methods developed to determine and manage cybersecurity risks while connecting to external systems with NAS stakeholders and users.
- Conduct analysis of the data captured to develop appropriate domain-dependent behavior baselines at various levels (enterprise, networks, specific systems, and devices) based on the domain requirements and time-history intervals.
- Develop analytical capabilities for aggregating and correlating current behavioral and operational data with the intent of understanding, predicting, and responding to cyber events.
- Develop cyber-testing capabilities that will help identify and quantify known risks.

4.2.3 Critical Milestones/Outputs

- FY18—Develop advanced big data analytics approaches to detect and respond to advanced persistent and insider threats.
- FY19—Develop initial cyber-testing capability to test, evaluate, and validate data analytic/visualization tools in an operational environment.
- FY20—Based on research findings and actual NextGen technology implementations, update a previously developed research roadmap to improve the FAA's capability in operating a mixed-trust, massively interconnected network of systems and external domains of different levels of security pastures and controls.
- FY21—Develop a systematic approach to continuously identify cybersecurity risk-based mission-critical equipment, and develop corresponding technology solutions of improved security postures.

4.2.4 Outcome

The NAS is an integral part of the nation's critical infrastructure as identified in PPD-21. Maintaining the continued operations of the nation's air traffic management systems and preventing interruptions of NAS functions are essential to provide the safest and most efficient travel system for the flying public. The outcomes of this research will enable the FAA to provide the necessary protections of the ATC services and associated functions from potential disruptive cyber events.

4.2.5 Funding Profile

	Year 1 2018	Year 2 2019	Year 3 2020	Year 4 2021	Year 5 2022
Funding	$1,000K	$1,000K	$1,000K	$1,000K	$1,000K

Status: A multi-year, ongoing R,E&D-funded requirement

4.3 Identity and Authorization Management Interoperability—Requirement

4.3.1 Description

The purpose of this research is to collaborate, assess, and analyze the expansion of identity and authorization management (IAM) with domestic and international public key infrastructure (PKI) systems, and to explore and recommend solutions for interoperability, capacity, and architectural issues that arise with the industry, domestic, and international aviation partners. Currently, there are significant gaps in knowledge, policy, and processes with respect to IAM interoperability in the heterogeneous environment that comprises the global community. Specifically, the research should investigate the interoperability of IAM with non-U.S. Common Policy compliant certificates in domestic use cases, and to investigate the use of IAM in interactions with international aviation stakeholders when Transportation Security Clearance Program (TSCP) or other non-US Common Policy alternatives must be used. The research should also investigate the use of an expanded set of algorithms and NSA-recommended "transition" algorithms, both within IAM and when interacting with external PKI. The research should also investigate an expanded internal use of IAM in non-system wide information management use cases, and investigate the use of IAM to support PIV authentication within the NAS.

4.3.2 Initiatives/Tasks

This requirement's research tasks investigate, assess, and provide recommendations for interoperability issues between IAM and external PKI—both domestic and international—and those using elliptic curve, an alternate algorithm of PKI. The research will guide IAM policy and interoperability guidance and procedures. The specific requirement tasks are to:

- Define, identify, and evaluate an expansion of IAM that supports internal system-to-system and human-to-system internal NAS use cases, to include performance and capacity constraints.
- Collaborate with domestic aviation stakeholders to identify and assess issues associated with the interoperability of IAM with domestic aviation stakeholders using PKI that are not directly U.S. Common Policy compliant.
- Identify and recommend policy and technical solutions to issues identified in the two previously mentioned tasks.

- Define, identify, and assess technical limitations of IAM with respect to interoperability with certificates that exceed the U.S. Common Policy requirements implemented by IAM in terms of strength, length, or algorithmic complexity.
- Collaborate with international aviation partners to identify and assess issues associated with the interoperability of IAM with international aviation stakeholders using PKI that are not directly U.S. Common Policy compliant, such as those using the TSCP.
- Develop an IAM Expansion architecture that addresses the needs of the heterogeneous environment defined and evaluated above.
- Develop an Operational Concept for an IAM expansion that addresses the interoperability, architectural, capacity, and performance necessary to support the expanded set of use cases defined herein from both an aviation industry perspective and an FAA perspective.

4.3.3 Critical Milestones/Outputs

- FY19—Development of requirements, architecture and Concept of Operations for IAM and PIV.
- FY20—Methodology for expanding IAM trust framework, algorithmic interoperability, and internal use cases, including collaboration with the expanded, heterogeneous IAM user community.
- FY21—Results from interoperability testing for domestic use case (Datacom, WiMAX, domestic aviation partners).
- FY22—Results from interoperability testing for international use case.
- FY23—Technical data for use in the development of standards, policies, and governance to support the unified global Operational Concept for IAM.

4.3.4 Outcome

The research outputs will provide insights into interoperability issues as well as technical and policy-mitigation strategies that would provide a basis for developing rulemaking, policy, guidance, standards, training, and tools for security.

4.3.5 Funding Profile

	Year 1 2018	**Year 2 2019**	**Year 3 2020**	**Year 4 2021**	**Year 5 2022**
Funding	$0K	$3,250K	$3,250K	$3000K	$1,000K

Status: Currently, not a funded requirement

4.4 Cybersecurity for UAS Integration – Research Need

UAS will soon require the services of the NAS to fly in controlled airspace with traditional aircraft. This will require data to be exchanged between the operators of UAS systems and ATC facilities. The existing NAS telecommunications infrastructure will need to be expanded to accommodate new connections, while continuing to ensure the safety and security of the NAS and other FAA systems. The proposed research is designed for larger UAS, which will be attempting to fly in Airspace Classes A–E, although accommodation of smaller cleared UAS will be explored to find the lower limit of aircraft capability to fly in controlled space.

Research will be required to create a realistic virtual representation of the existing NAS and FAA Telecommunications Infrastructure (FTI) systems and add a new communications portal and UAS end systems.

Figure 4 shows the environment that will be created to model various characteristics of a future UAS to NAS portal. The actual portal components are depicted in green and provide a common interface to UAS owners and operators. The UAS depicted at the top of the diagram are intended to be simple simulations designed to provide a wide variety of nominal and non-nominal data flows to fully exercise the capabilities of the proposed communications infrastructure. The lower blue and brown portions are virtual simulations of existing NAS infrastructure to also provide the ability to measure the security and performance of the portal under a variety of conditions. The tasks, milestones, research outcomes, and resources required will be provided in a future update to the R&D plan.

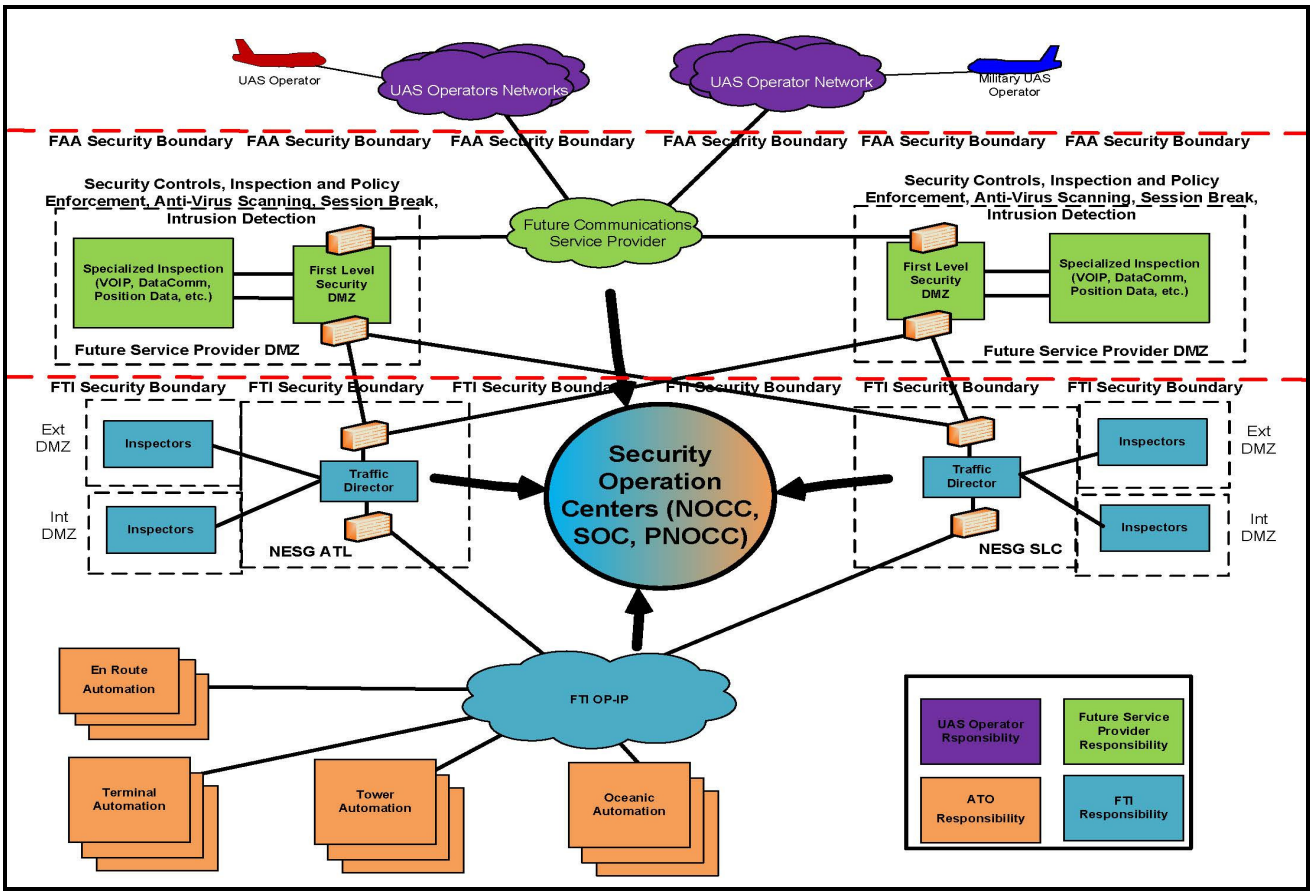

Figure 4: Cybersecurity for UAS Integration Model

5.0 Research Area–Human Behavior/Human Factors

Develop and validate human-in-the-loop policies, training, and procedures to detect and respond to cyber-attacks.

5.1 ASISP Response and Recovery–Requirement

5.1.1 Description

An aircraft is a complex control system. To accurately quantify the safety risk of an information security attack, it needs to be determined whether aircraft pilots will recognize that a cyber-attack is occurring and, if so, respond appropriately. In particular, a cyberattack may result in pilot behavior similar to that previously observed when there is a system failure, and, therefore, it would be important to first understand how the results of the current literature regarding trust, mistrust, and over-trust are applicable to this situation.

The approach to this research would be to examine the research literature and, if necessary, design and conduct research studies in which specific cyber-attack scenarios would be presented with the goal of gathering quantitative data to understand pilot behavior.

The results of this analysis would provide data to understand the human-factors implications of an information security attack.

5.1.2 Initiatives/Tasks

- Coordinate with other research organizations (e.g., Department of Defense [DOD], NASA, etc.) to gather data to understand the spectrum of applicable cyber-risk scenarios, aircraft equipment, and capabilities required to generate the cyber-attacks.
- Review the literature to determine what research has been conducted in this area.
- If necessary, modify existing and selected simulation capabilities to enable simulation of cyber-attack scenarios.
- Design and conduct research studies with pilots.

5.1.3 Critical Milestones/Outputs

- FY20—Results of literature review identifying research gaps specific to information security.
- FY21—Develop research plan to address the research gaps. Enhanced laboratory response and recovery capabilities to conduct simulation of various cyber-attack scenarios.

- FY22—Conduct and analyze results of research studies.

5.1.4 Outcome

The results of ASISP response and recovery simulations will provide quantifiable data and provide a basis for the Office of Aviation Safety (AVS) to evaluate the accuracy of the analytical risk assessment results in ASISP. The ASISP response and recovery simulations will further provide AVS with validated human factors data and context to study pilot responses to cyber-attacks in regard to piloting tasks and workload levels. The results of ASISP response and recovery simulations shall also be used to develop additional rulemaking, policy, guidance, standards, training, and support tools that are not being addressed through the ASISP research requirement.

5.1.5 Funding Profile

	Year 1 2018	**Year 2 2019**	**Year 3 2020**	**Year 4 2021**	**Year 5 2022**
Funding	$0	$0K	$1,000K	$1,500K	$1,500K

Status: Currently not a funded requirement

5.2 Situational Awareness Visualization, Threat Assessment, and Compliance - Requirement

5.2.1 Description

The NAS today is protected against threats by a variety of architectural and technical controls that focus on protecting against external threats. Firewalls; demilitarized zones; traffic analysis and inspection; malware protection; and a host of other controls seek to prevent intruders from breaching the NAS and weakening its confidentiality, integrity, and availability. Recent history suggests that an external focus is inadequate to meet the full scope of threats faced by today's information systems. The Federal Information Security Management Act (FISMA) mandates government agencies to operate an information security program in compliance with NIST Special Publication 800-53. The FAA, through FAA Order 1370.121, has implemented a comprehensive Information Security Continuous Monitoring (ISCM) program that meets the requirements of FISMA through continuous monitoring, periodic vulnerability assessment, aggressive Plan of Actions and Milestones item remediation, and annual accreditation. While these measures all work together to improve the security posture of the FAA, gaps exist in the information collected and in the association of such information to systems and controls. The purpose of this research is to identify and assess products that can assist the FAA in the detection, protection, behavior analysis, and visualization of insider threats, and to support the requirement for ISCM. The following types of tools will be addressed through this requirement:

- "Insider threat" and an integrated visualization and analytic tool set

- Behavior analysis tools
- Threat assessment tools that integrate with the situational awareness to provide a real-time snapshot of our threats
- Real-time assessment of the functional domains to assess the agency's compliance with NIST

5.2.1 Initiatives/Tasks

The research tasks for this requirement identify, integrate, evaluate, and provide recommendations for products that enhance the situational awareness visualizations available to operators and maintainers of the NAS. This research will guide FAA policy and procedures related to internal threat detection and prevention. The specific requirement tasks are to:

- Identify and assess tools currently implemented within the NAS that, when extended, can support situational awareness of internal threats to the NAS.
- Identify and assess additional tools that would augment situational awareness and provide visualizations of internal threats to the NAS.
- Implement and evaluate the compatibility, usability, capability, and interoperability of additional tools identified in the previous task.
- Identify and assess additional tools that would augment threat assessment and compliance, provide real-time compliance monitoring, and collect and incorporate threat intelligence.
- Evaluate potential impacts of the use in FAA domains of tools evaluated previously on network utilization and performance, and personnel impacts to training and staffing requirements that could result from the use of such tools in the NAS.
- Define, implement, and evaluate potential mitigations to the impacts identified previously.
- Identify and recommend specific tools, policy, architecture, and technical solutions for potential implementation of tools evaluated in the previous tasks.

5.2.3 Critical Milestones/Outputs

- FY19—Initial survey of tools currently deployed in the NAS and market survey of additional tools that support situational awareness visualization.
- FY19—Methodology for the implementation, integration, and evaluation of additional tools.
- FY19—Assessment of candidate situational awareness visualization, real-time threat assessment and compliance tools, and threat intelligence tools in the R&D domain.
- FY21—Implementation and post-evaluation of selected tools and impact mitigations in the R&D domain.
- FY22—Proposed set of recommendations for implementation of situational awareness visualizations and threat compliance, threat assessment, and threat intelligence within the FAA.

5.2.4 Outcome

The research outputs will provide guidance and recommendations on tools that are available to support situational awareness visualizations, how they can be integrated into the NAS, and how potential impacts to the NAS can be mitigated. These outputs will provide a basis for developing guidance, standards, training, and tools for potential acquisition and implementation of situational awareness visualization tools.

5.2.5 Funding Profile

	Year 1 2018	**Year 2 2019**	**Year 3 2020**	**Year 4 2021**	**Year 5 2022**
Funding	$0K	$1,000K	$2,000K	$1,500K	$500K

Status: Currently not a funded requirement

6.0 Research Area—System wide Safety Assurance

Develop real-time, continuous safety analysis and assurance tools and capabilities to prevent/mitigate the impact of cyber-attacks.

6.1 FAA Cybersecurity Test Facility Virtualization—Requirement

6.1.1 Description

The primary objective of the Cybersecurity Test Facility (CyTF) is to be the test bed for conducting enterprise tests; evaluations and validations of security products; and processes and services prior to integration into the four FAA domains. CyTF provides a cost-effective and safe testing environment for validating the FAA's cybersecurity risk model and performing cybersecurity exercises. The CyTF also provides the ability to prototype complex enterprise security capabilities and solutions and exploit vulnerabilities without impacting other FAA activities.

6.1.2 Initiatives/Tasks

The research requirement is to identify, evaluate, and provide recommendations for candidate systems and tools that should be virtualized for use within the CyTF. In addition, tasks include collaboration with industry partners and other government agencies to conduct joint research and evaluation for applicability to the FAA environments. This research will guide the evolution of the CyTF to provide more comprehensive and complex cybersecurity exercises, product evaluations, cybersecurity risk testing, and other R&D activities. The specific requirement tasks are to:

- Identify and assess the FAA domain capabilities that are suitable for inclusion within the CyTF and have the potential to further the mission of the CyTF.
- Define the methodology, and virtualize, integrate, and validate the capabilities identified in the previous task.
- Conduct joint cybersecurity capabilities research, development, and engineering with industry partners and other agencies for FAA applicability, and enhance the FAA advance solution tool set.
- Define, identify, and assess cybersecurity vulnerabilities in the R&D domain, and recommend mitigation strategies.

Note that these tasks are envisioned as annually recurring tasks to provide for continually evolving and improving the CyTF capability.

6.1.3 Critical Milestones/Outputs

- FY19—Results from an initial survey of FAA domain capabilities already available within the CyTF. Identification of candidate FAA domain capabilities for inclusion into the CyTF.
- FY20—Virtualization and integration of candidate capabilities into the CyTF.
- FY21—Evaluation of cybersecurity capabilities from industry and other agencies.
- FY21—Assessment of improved CyTF capabilities and functionalities.
- FY22—Identification of additional candidate FAA capabilities for inclusion into the CyTF.
- FY22—Assessment of domain vulnerabilities against the R&D domain and recommendations for mitigation strategies.

6.1.4 Outcome

The research outputs will provide continual improvement and enhancement of the CyTF capabilities, and enable comprehensive, realistic, and complex cybersecurity exercises, product evaluations, and other R&D activities.

6.1.5 Funding Profile

	Year 1 2018	Year 2 2019	Year 3 2020	Year 4 2021	Year 5 2022
Funding	$0K	$1,500K	$1,500K	$1,000K	$1,000K

Status: Currently not a funded requirement

6.2 UAS Security Control Capability—Requirement

6.2.1 Description

The proposed research addresses communications security needed to maintain a resilient security framework for implementing communication security controls for new and unique terrestrial, SatCom, and network terrestrial and SatCom C2 data link systems. This proposed research will conduct in-house testing to assess efficient and effective mitigation against security threats of terrestrial, SatCom, and network terrestrial and SatCom C2 data-link systems with a high level of sophistication.

6.2.2 Initiatives/Tasks

- Establish an in-house lab capability to conduct the research, prototype, and validation testing.

- Conduct in-house lab testing to assess and validate efficient and effective mitigation against security threats of terrestrial, SatCom, and network terrestrial and SatCom C2 data-link systems with a high level of sophistication.

6.2.3 Critical Milestones/Outputs

- FY22—Development of avionic systems-design and airworthiness-approval requirements for the UAS C2 CNPC data links.

6.2.4 Outcome

This research directly supports the ongoing RTCA SC-228 standards development by the UAS community, AVS for C2 terrestrial, SatCom, and networked C2 Link Systems security protection. This research also directly supports the development of FAA new TSO requirements and AC guidance for security protection of new and unique C2 terrestrial, SatCom, and networked systems, FAA Path Finder certification activities, publication of operational guidance materials, and other related activities.

6.2.5 Resources

Resource Table

	Year 1 2018	Year 2 2019	Year3 2020	Year 4 2021	Year 5 2022
Funding	$400K	$600K	$600K	$0K	$0K

Status: Approved multi-year R,E&D requirement that is planned to be initiated in FY18

6.3 Analysis of Unmanned Aircraft-Control Station Ground-to-Ground Communication with the NAS ATC—Research Need

The FAA UAS Technical Community Requirements Group has identified ground-to-ground voice telecommunication infrastructure as an area of interest and a building block towards certifying and formulizing UAS operations.

Currently, communication between ATC and pilots is handled by an aging analog voice infrastructure that has reached the end of its sustainable lifecycle. The NAS voice system (NVS) will replace the current set of voice switches with a Voice over Internet Protocol (VoIP)- based digital infrastructure. NVS VoIP Services will use FTI as transport and will be operated as part of the NAS. The use of VoIP will standardize voice communications among air traffic facilities and allow a great degree of flexibility for routing voice communications within the NAS.

Any system or application external to the NAS that communicates via IP with a system or application within the NAS must pass through the NAS Security boundary. The NAS Security boundary is composed of four NAS Enterprise Security Gateways (NESGs), as defined in the JO 1370.114 Implementation of FAA Telecommunications Infrastructure Services.

The four NAS NESGs have been deployed to be the focal points of communication between NAS and non-NAS. Each NESG contains a variety of security appliances that enforce access control lists, perform deep-packet inspection, address network address translation requirements, and scan the incoming traffic for malicious payloads.

This research will identify the safety issues associated with the use of UAS gateways that provide the capability for multiple pilots-in-command (PICs) to communicate with ATC via dynamically built voice bridges. The concept of a UAS gateway is required to replicate the existing RF capability to host multiple pilots that can all simultaneously communicate with ATC. Similar to a radio that broadcasts to all aircraft within range and on the same frequency, the UAS gateway transmits the controller voice to all UAS PICs connected to the gateway voice bridge corresponding to the airspace. The tasks, milestones, research outcomes, and resources required will be provided in a future update to the R&D plan.

6.4 Cyber Positioning, Navigation, and Timing—Research Need

Space-based positioning, navigation, and timing (PNT) provided by the U.S. GPS and its FAA augmentations have an increasingly important role as enabling technologies for NextGen capabilities and are a potential critical, common-mode failure mechanism for essential elements of the national airspace infrastructure and external supporting infrastructure sectors. In spring 2017, the FAA incorporated the DHS Best Practices for operation and development of GPS equipment used in critical infrastructure into the FAA TSOs for GPS equipment. The FAA is working with DHS S&T to access the vulnerabilities of GPS equipment, including timing systems used in NAS infrastructure. Additionally, the FAA GPS Intentional Interference and Spoofing Study Team is preparing a research plan to assess cyber-data spoofing of GPS time effects on FAA automation, communications, navigation, surveillance, and weather systems. When possible, these activities will be conducted jointly with DHS and other agency partners. The tasks, milestones, research outcomes, and resources required will be provided in a future update to the R&D plan.

7.0 Technical Collaborations

This section maps to the Cybersecurity Strategic Plan Goal 5 (i.e., Build and Maintain Relationships With External Partners in Government and Industry). The FAA will work closely with partners, both government and industry, to improve and leverage information, communications, preparation, and defense actions needed to protect FAA systems and networks.

7.1 Process

Before any R&D project can begin exploring new ideas, technologies, methodologies, and capabilities, the agency will solicit input from partner agencies to identify and plan cyber R&D projects that potentially will yield benefits to all. Appendix D provides a brief description of the collaboration process used by the agency.

7.2 Multiagency R&D Synchronization

7.2.1 Other Agencies

The increasing interconnectivity and complexity in the aviation ecosystem brings the reality that all affected stakeholders need to practice technical collaborations with partners to share and exchange research ideas, technologies, tools, and techniques. While the FAA's cybersecurity R&D collaboration with other agencies is evolving, the FAA and its NextGen partner agencies conducted workshops and technical exchanges in Fiscal Year 2015 and Fiscal Year 2016 to identify R&D needs and gaps and analyze partner agencies' cybersecurity R&D portfolios for potential transition to practice. Partner agencies include the FAA, DHS, Office of the Director of National Intelligence, DoD, NASA, and Department of Commerce. The Interagency Cyber Core Team (ICCT), which the FAA Interagency Planning Office for NextGen established under the auspices of the NextGen Executive Board, led this collaborative effort. In partnership with the DHS, DoD, and Department of Justice, the FAA administrator also signed the Commercial Aviation Cybersecurity Task Force Charter that directed an interagency Aviation Cybersecurity Initiative (ACI), including an R&D effort for aircraft cyber evaluation to investigate and evaluate aircraft cybersecurity vulnerabilities.

Leveraging existing FAA and interagency R&D processes and mechanisms, the FAA will continue to pursue and participate in technical collaborations with partner agencies throughout the entire cybersecurity R&D lifecycle. This includes brainstorming ideas; identifying requirements; formulating concepts; planning, proposing, and conducting research; fostering technical exchanges; and transitioning tools and technologies into operations.

The following describes FAA cybersecurity R&D collaborations with partner agencies:

- NextGen partner agencies formed the ICCT to facilitate interagency collaboration in aviation cybersecurity. The ICCT has two focus areas—Cyber Exercises and Cyber R&D. The Cyber Exercise focus area engages in federally sponsored exercises, such as Cyber Guard, to identify potential vulnerabilities in aviation systems and to inform the Cyber R&D focus area for further R&D. Additionally, the Cyber R&D focus area conducts periodic workshops to identify unmet aviation cybersecurity gaps/needs and to regularly survey federally sponsored Cyber R&D that might address these gaps/needs. As advanced technologies evolve, the Cyber R&D focus area assesses and evaluates their impact on the aviation ecosystem.

- The FAA is also working with the DHS and DoD on the ASISP cyber initiative in support of AVS. The goal of this multi-year research effort is to develop a cybersecurity safety risk management process that would continuously provide data, analysis, and recommendations to FAA decision-makers to support policy and regulatory decisions and to coordinate and collaborate with the aviation industry to both address and continuously assess aircraft cyber-risks associated with aviation safety.

- NextGen partner agencies, led by the DHS, is conducting the ACI R&D project, a multi-year research effort that is designed to examine various cybersecurity vulnerabilities in aircraft and avionics systems and recommend mitigation strategies. The goal is to clearly identify and articulate the various systems' cybersecurity vulnerabilities and work with the interagency partners, academia, and industry to develop mitigation strategies and solutions. The research plan is scalable and can accommodate any number of systems tests using the test article aircraft located at the FAA William J. Hughes Technical Center in Atlantic City, NJ. The ACI R&D and ASISP R&D projects (section 2.3) complement each other to establish repeatable and verifiable risk-management practices for aircraft cybersecurity. Some of the systems to be evaluated include but are not limited to the electrical system, flight management system, and full-authority digital engine (electronic) control system.

- Cybersecurity R&D collaboration is an ongoing process that employs continual technical exchanges among all stakeholders to ensure that relevant research efforts are shared to address critical aviation cybersecurity risks. The scope of technical exchanges includes not only operational and research tools and technologies, but also models, architecture, standards, and engineering principles. The partner agencies, as a general rule, will hold periodic technical exchange meetings to ensure that principal investigators and researchers share and exchange research ideas and technical information on their R&D projects.

- The FAA is working with NASA, the DoD, and the DHS to formulate a joint research effort, Secure Net-centric Aviation Communication (SNAC) R&D, which would research

concept, architecture, and technologies for future aviation communication requirements. The SNAC vision is to deliver a new dimension of situational awareness, decision support, safety, and security for all participants in the aviation ecosystem. SNAC is an operational concept for future aviation communication that provides always-on, secure, flexible, routable, and resilient information service between aircraft, aircraft and the ground, and aircraft and space assets. Envisioning participants as a node in a secure network, capable of sending and receiving critical data through application of network connectivity methods, protocols (rules), security technologies, and robust capacity, SNAC will use all available link technologies (radio, satellite, terrestrial) in the operational environment to deliver information to all participants in the aviation ecosystem.

- In August 2016, DHS S&T issued the "Assured Timing for Critical Infrastructure" Broad Area Announcement (BAA) to support development of assured timing technologies, system-level testing, and analysis to understand system impacts and the development of timing manipulation and data-spoofing detection capabilities. In December 2016, the Executive Office of the President released an infrastructure security and resilience implementation roadmap that calls for PNT[2] R&D planning and investments to address PNT cyber-threats.

- In December 2016, the National Defense Authorization Act (NDAA) tasked all "covered Secretaries" (including the Secretary of Transportation) to "jointly conduct a study to assess and identify the technology-neutral requirements to backup and complement the position, navigation, and timing capabilities of the GPS for national security and critical infrastructure." In January 2017, the DHS Office of Infrastructure Protection released a Best Practices document to address operation and development of GPS equipment used by critical infrastructure. This document included a section on research opportunities to enhance resilience in civilian infrastructure use of GPS and addresses GPS cyber-data spoofing mitigations to make our applications more robust, including expanded use of independent systems. Currently, DHS S&T is executing the BAA, and DHS, DOT, and the DoD are working together to address the timing tasking in the NDAA and to implement the GPS Best Practices recommendations.

- Space-based PNT provided by the U.S. GPS and its FAA augmentations have an increasingly important role as enabling technologies for NextGen capabilities and are a potential critical, common-mode failure mechanism for essential elements of the national airspace infrastructure and external supporting infrastructure sectors. In spring 2017, the FAA incorporated the DHS Best Practices for operation and development of GPS-equipment used in critical infrastructure into the FAA TSOs for GPS equipment. The

[2] Implementation Roadmap For The National Critical Infrastructure Security And Resilience Research And Development Plan, Executive Office Of The President National Science And Technology Council, December 15, 2016.

FAA is working with DHS S&T to access the vulnerabilities of GPS equipment, including timing systems used in the NAS infrastructure. Additionally, the FAA GPS Intentional Interference and Spoofing Study Team is preparing a research plan to assess cyber-data spoofing of GPS time effects on FAA automation, communications, navigation, surveillance, and weather systems. When possible, these activities will be conducted jointly with DHS and other agency partners.

- In spring 2017, the FAA incorporated the DHS Best Practices for operation and development of GPS equipment used in critical infrastructure into the FAA TSOs for GPS equipment. The FAA is working with DHS S&T to access the vulnerabilities of GPS equipment, including timing systems used in the NAS infrastructure. Additionally, the FAA GPS Intentional Interference and Spoofing Study Team is preparing a research plan to assess cyber-data spoofing of GPS time effects on FAA automation, communications, navigation, surveillance, and weather systems. When possible, these activities will be conducted jointly with DHS and other agency partners.

7.2.2 Industry

The Cooperative Research and Development Agreement (CRDA) is one of the principle mechanisms used by federal laboratories to engage in collaborative efforts with partners to achieve the goals of technology transfer. CRDAs support the broader purpose of providing the means for a laboratory/agency to leverage its R&D efforts, consistent with the agency's mission. The FAA supports the development of CRDAs that encourage the creation of interdisciplinary teams from across the industry and government to address the most challenging cybersecurity issues impacting the aviation industry. As an example, figure 5 shows the various critical partnerships in which the requirements contained in this plan are engaged to identify information-security-protection vulnerabilities and risks that are required to prevent, detect, and react to cyber-attacks, and to safely secure FAA NAS and mission support infrastructure.

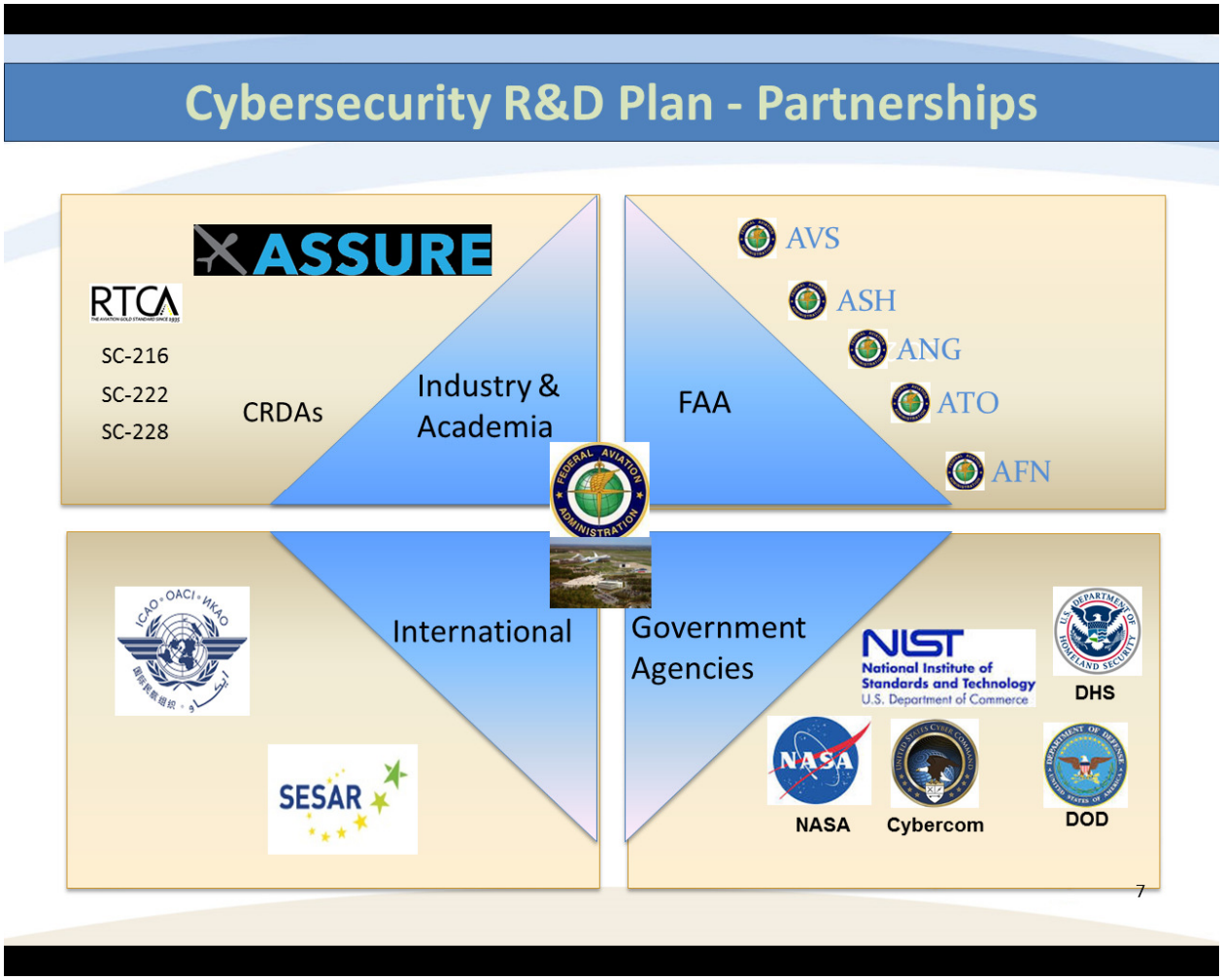

Figure 5: Industry/Academia Collaboration

7.2.3 Academia

The goal of technology transfer is the sharing among federal laboratories and academia to include not only technologies, but also personnel, facilities, methods, expertise, and technical information in general. The FAA encourages the development of Centers of Excellence (COEs) with academic institutions. The COE program facilitates collaboration and coordination between government, academia, and industry to advance aviation technologies and expand FAA research capabilities through congressionally required matching contributions. The COEs are established through cooperative agreements with the nation's premier universities, and their members and affiliates, who conduct focused R&D and related activities over a period of 10 years. As an example, FAA's COE for UAS research, Alliance for System Safety of UAS Through Research Excellence (ASSURE) include 23 of the world's leading research institutions and 100 leading industry, government partners addressing some of the most challenging UAS research needs, including that of cybersecurity.

7.2.4 International

The FAA coordinates with the ICAO Communications Panel–Data Communications Infrastructure Working Group. As the contributing member of the CP, the FAA developed Standards and Recommended Practices (SARPs) and guidance materials for air-ground and ground-ground aeronautical communications, including both voice and data.

These SARPs and policies are used by ICAO member states to ensure that their local civil aviation operations and regulations conform to global norms, which in turn permit more than 100,000 daily flights in aviation's global network to operate safely and reliably in every region of the world.

The FAA shall also leverage previous experience working in the ICAO Communications Panel, RTCA SC-228, and with AIR-130 to develop the security provisions for the Phase Two C2 Data Link MOPS and an associated AC. The FAA shall further support RTCA SC-228 and AIR-130 in developing the Phase One "Command and Control (C2) Data Link MOPS (Terrestrial)" as published in RTCA-DO-362 and in developing the Draft AC "Airworthiness Approval of UAS CNPC Terrestrial Link Systems" (AC No: 20-187).

Additionally, the FAA NextGen office engages in international cybersecurity research with the Single European Sky ATM Research (SESAR) Joint Undertaking office. This body of work is conducted under the U.S.-European Commission Memorandum of Cooperation (MOC) for ATM R&D. The MOC with SESAR defines "Work Areas" for collaboration and specifies that all work will be captured in work plans with leaders assigned from both the FAA and the SESAR Joint Undertaking. In 2016, the FAA and SESAR Joint Undertaking created a new work plan for cybersecurity collaboration, connected to NextGen and SESAR R&D efforts. The scope and details of the cybersecurity work plan are currently under negotiation between the FAA and SESAR Joint Undertaking Office. The agency expects to have a work plan ready for signature in September 2017. Although the work will be focused on R&D activities, the degree of collaboration will be limited by the constraints placed on SESAR Joint Undertaking because they are not the primary cybersecurity organization in the European Commission.

8.0 Funding Summary

Table 1 - Cybersecurity R&D Plan Funding Summary

Requirement	Research Area	2018 Requested	2019 Planned	*2020 Estimate*	*2021 Estimate*	*2022 Estimate*
ASISP	Security & Resiliency	$2,000K	$2,100K	*$2,600K*	*$2,200K*	*$2,000K*
Cybersecurity Risks of Cabin Communications and Cabin IT Systems	Security & Resiliency	$0K	$2,000K	*$2,000K*	*$2,000K*	*$2,000K*
UAS Networked C2 Link Systems Security Protection	Security & Resiliency	$310K	$330K	*$350K*	*$0K*	*$0K*
Flight Deck Data Exchange	Data Analytics	$0	$2,000K	*$2,100K*	*$2,200K*	*$2,200K*
NextGen-Information Security	Data Analytics	$1,000K	$1,000K	*$1,000K*	*$1,000K*	*$1,000K*
IAM Interoperability	Data Analytics	$0K	$3,250K	*$3,250K*	*$3,000K*	*$1,000K*
ASISP Response and Recovery	Human Behavior/ Human Factors	$0K	$0k	*$1,000K*	*$1,500K*	*$1,500K*
Situational Awareness Visualization, Threat Assessment and Compliance	Human Behavior/ Human Factors	$0K	$1,000K	*$2,000K*	*$1,500K*	*$500K*
UAS Security Control Capability	Systemwide Safety Assurance	$400K	$600K	*$600K*	*$0K*	*$0K*
CyTF Virtualization	Systemwide Safety Assurance	$0	$1,500K	*$1,500K*	*$1,000K*	*$1,000K*
Total		**$3,710K**	**$13,780K**	***$16,400K***	***$14,400K***	***$11,200K***

Table 2 - Cybersecurity R&D Funding Profile by Research Area

Research Area	FY 18 Requested	FY19 Planned	*FY20 Estimate*	*FY21 Estimate*	*FY22 Estimate*
Security & Resiliency	$2,310K	$4,430K	*$4,950K*	*$4,200K*	*$4,000K*
Data Analytics	$1,000K	$6,250K	*$6,350K*	*$6,200K*	*$4,200K*
Human Behavior/Human Factors	$0	$1,000K	*$3,000K*	*$3,000K*	*$2,000K*
System Wide Safety Assurance	$400	$2,100K	*$2,100K*	*$1,000K*	*$1,000K*

Appendix A: Acronyms

AC	Advisory Circular
ACI	Aviation Cybersecurity Initiative
AIT	FAA Information and Technology
ASISP	Aircraft Systems Information Security Protection
ATC	Air traffic control
ATM	Air Traffic Management
AVS	Office of Aviation Safety
BAA	Broad Area Announcement
BLOS	Beyond line of sight
C2	Command and control
CEO	Chief executive officer
COE	Center of Excellence
CNPC	Non-payload communications
CRDA	Cooperative Research and Development Agreement
CSC	Cybersecurity Steering Committee
CyTF	Cybersecurity Test Facility
DHS	Department of Homeland Security
DoD	Department of Defense
FISMA	Federal Information Security Management Act
FTI	FAA Telecommunications Infrastructure
GPS	Global Positioning System
IAM	Identity and authorization management
ICCT	Interagency Cyber Core Team
ISCM	Information Security Continuous Monitoring
IT	Information technology
MOC	Memorandum of Cooperation
MOPS	Minimum Operational Performance Standards
NAS	National Airspace System
NESG	NAS Enterprise Security Gateway
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NVS	NAS voice system
PIC	Pilot-in-command
PKI	Public key infrastructure
PNT	Positioning, navigation, and timing
PPD	Presidential Policy Directive
R&D	Research and development
RF	Radio frequency
RTCA	Radio Technical Commission for Aeronautics
S&T	Science and technology
SARPs	Standards and recommended practices
SESAR	Single European Sky ATM Research
SNAC	Secure Net-centric Aviation Communication
SRA	Safety risk assessment
TBO	Trajectory Based Operations
TRL	Technical readiness level

TSCP	Transportation Security Clearance Program
TSO	Technical Standards Order
UAS	Unmanned aircraft system(s)
VoIP	Voice over Internet Protocol

Appendix B: Cybersecurity Goals: 2017–2022

Core Cybersecurity Goals 2017-2022 Governance • Vulnerability Management • Security Architecture, Policy, and Standards • Systems and Applications Security • Continuous Diagnostics and Monitoring • Security Operations				
Goal 1	**Goal 2**	**Goal 3**	**Goal 4**	**Goal 5**
Refine and maintain a cybersecurity governance structure to enhance cross-domain synergy	Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery	Enhance data-driven risk management decision capabilities	Build and maintain workforce capabilities for cybersecurity	Build and maintain relationships with external partners in Government and industry to sustain and improve cybersecurity in the aviation domain
Objectives	**Objectives**	**Objectives**	**Objectives**	**Objectives**
1.1 Maintain cross-organization processes for cybersecurity strategic planning and budget development 1.2 Codify and maintain FAA-wide Cybersecurity Roles & Responsibilities 1.3 Improve understanding of cybersecurity risk for FAA owned, contracted and regulated systems 1.4 Increase integration of cybersecurity activities across Domains 1.5 Update and maintain FAA-wide information security policies	2.1 Improve cyber threat intelligence collection, processing, dissemination, and reporting 2.2 Improve FAA cyber monitoring, detection and response capabilities 2.3 Improve privileged user control, monitoring and visibility 2.4 Improve capabilities for detection and mitigation of threats, internal and external 2.5 Leverage cybersecurity research and development across FAA domains and systems 2.6 Ensure FAA Information Security Controls, Policies and Processes are aligned with current NIST Standards and Guidelines	3.1 Continue development and enhancement of an enterprise cyber threat modeling capability 3.2 Expand Information Security Continuous Monitoring capabilities for NAS and non-NAS IP systems 3.3 Integrate threat, attack and vulnerability data with mission focus to prioritize risks 3.4 Reduce the time required to address high value threats and vulnerabilities	4.1 Enhance FAA-wide cybersecurity training, education and awareness program 4.2 Support cyber workforce training through participation in exercises 4.3 Ensure personnel having cybersecurity responsibilities receive appropriate role-based training 4.4 Enhance FAA competitiveness in cybersecurity hiring and retention through adoption of current Federal IT Job Series	5.1 Expand participation in cyber exercises with external partners 5.2 Increase collaboration with other Government, industry and private sector cybersecurity teams 5.3: Ensure cybersecurity requirements are addressed in the AMS and all FAA contract vehicles (ACQ) 5.4 Expand information sharing with appropriate external partners including through automated cyber threat indicator sharing 5.5 Leverage regulatory role to identify and address cybersecurity risks in aircraft systems as well automation of aircraft, equipment and technology 5.6 Represent the United States in global engagement on aviation cybersecurity through partnership and engagement with international partners

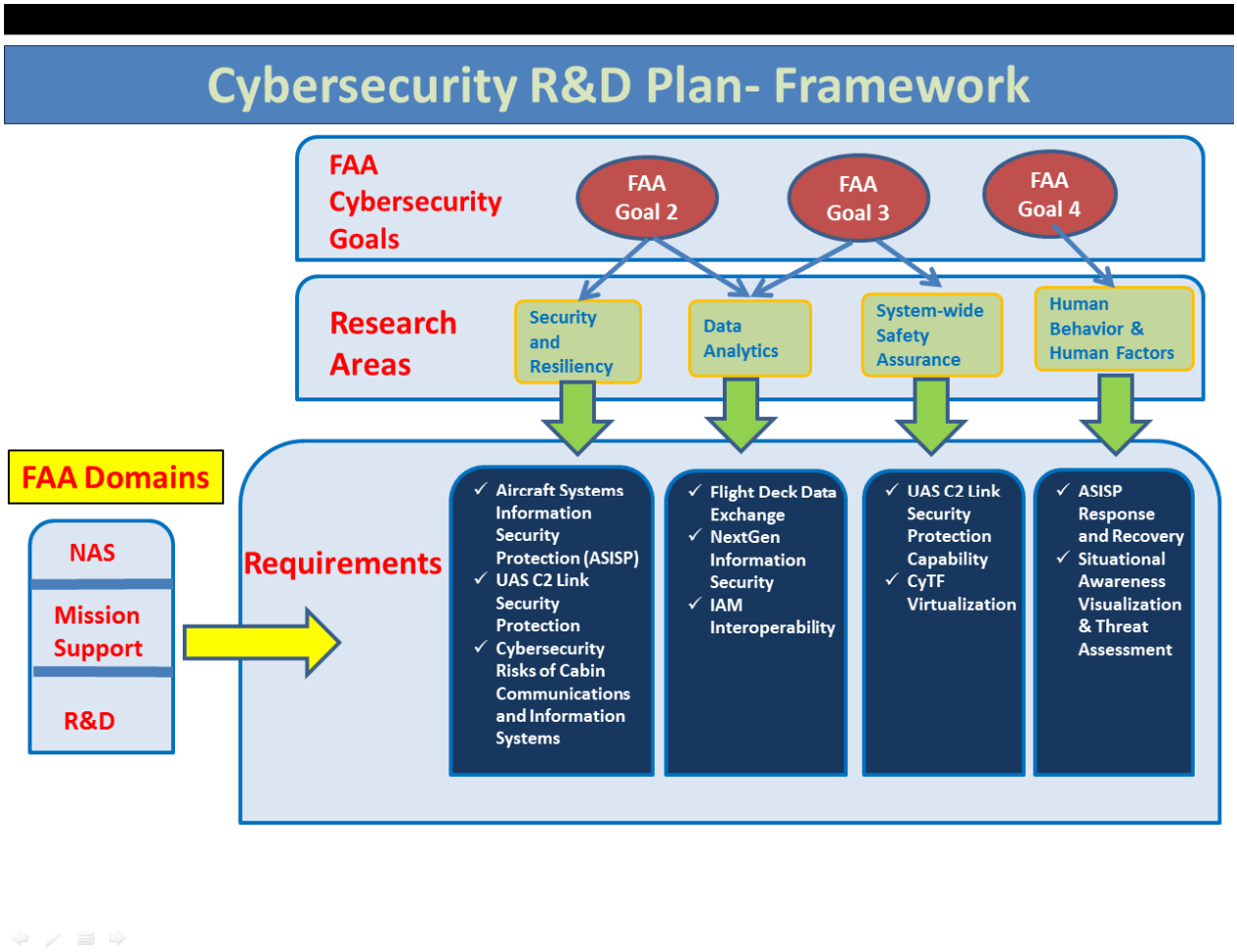

Figure B-2: Cybersecurity R&D Plan- Framework

Table B-1: Cybersecurity Research Requirements Categorization by FAA Domain/Research Area

		Primary Domain		
Requirement	**Research Area**	**NAS**	**R&D**	**Mission Support**
ASISP	Security & Resiliency			Regulatory Service
UAS C2 Link Security Protection	Security & Resiliency			Regulatory Service
Cybersecurity Risks of Cabin Communications and Cabin Information Technology Systems	Security & Resiliency			Regulatory Service
Flight Deck Data Exchange	Data Analytics	X		
NextGen Information Security	Data Analytics	X		
IAM Interoperability	Data Analytics		X	
UAS C2 Link Security Protection Capability	System wide Safety Performance		X	
CyTF Virtualization	System wide Safety Performance		X	
ASISP Response and Recovery	Human Behavior/Human Factors			Regulatory Service
Situational Awareness Visualization and Threat Assessment	Human Behavior/Human Factors	X		

UAS=unmanned aircraft system; ASISP=Aircraft Systems Information Security Protection; IAM=identity and authorization management; CyTF=Cybersecurity Test Facility; C2=command and control

Appendix C: Technical Collaboration Process

Before any research and development (R&D) project can begin exploring new ideas, technologies, methodologies, and capabilities, the agency will solicit input from partner agencies to identify and plan cyber R&D projects that will potentially yield benefits to all.

Cybersecurity Needs/Gaps Assessment

As cybersecurity threats to the aviation ecosystem continue to evolve and change, partner agencies will regularly assess and prioritize gaps and challenges and formulate requirements for new technology/solutions to address them. The product of the cybersecurity needs/gaps assessment will be a set of requirements that will inform planning and prioritization of R&D projects. To maximize return on investment, the participating agencies will share information and requirements with their partners to identify opportunities for cybersecurity R&D collaboration.

Cybersecurity R&D Portfolio Analysis

The partner agencies each have a portfolio of ongoing and planned cybersecurity R&D projects at various levels of maturity, measured in terms of technical readiness level (TRL). For partner agencies to have an opportunity to leverage partners' high TRL R&D projects, the team will conduct periodic portfolio reviews of cybersecurity R&D projects of each agency. The team will use the cybersecurity requirements discussed in the previous section as selection criteria to identify the R&D projects with the greatest potential to satisfy the requirement(s) and to yield benefits for one or more of the partner agencies. The team will examine each agency's portfolio of R&D projects and publish a summary report of the R&D projects that are most applicable to the cybersecurity requirements for the partner agencies to share. The primary target of the analysis will include cyber R&D portfolios of the FAA NextGen Office, Department of Homeland Security Science and Technology Directorate, Department of Defense Air Force Research Laboratories, and the NASA Aeronautics Research Mission Directorate.

Joint Cybersecurity R&D Proposal

NextGen partner agencies will collaborate to develop proposals to procure the resources necessary to address cybersecurity requirements that partner agencies identify as shared challenges/opportunities. The R&D project proposal will identify the specific cybersecurity requirement(s)/problems to be researched and the metrics upon which a positive outcome will be determined. Viable new technology/solutions resulting from the R&D project will be available for integration into the partner agencies' operational environment according to each agency's acquisition management practices.

Approach

The approach the agency is following includes the following:

- Conduct annual cybersecurity needs/gaps analysis with partner agencies.
- Translate needs/gaps into cybersecurity requirements that will drive cybersecurity R&D planning.
- Review partner agencies cybersecurity R&D portfolios.
- Identify high TRL R&D projects that address partner agencies' cybersecurity requirements.
- Develop joint proposal for cybersecurity R&D.

Outputs

The agency will jointly produce a Multiagency Cybersecurity R&D Analysis report that will be updated annually.

Outcomes

The following outcomes are anticipated:

- The partner agencies will have an understanding of shared cybersecurity needs/gaps on which to define requirements for subsequent cybersecurity R&D planning and prioritization.

- Partner agencies will share the most up-to-date knowledge of each other's cybersecurity R&D projects, thereby increasing the potential to maximize benefits gained from implementing the results of the most promising R&D projects.

- The partner agencies will realize the benefits of joint cybersecurity R&D with faster turnaround time from proposal development to technology/solutions realization. The most promising R&D results will be available for all partner agencies to implement to safeguard their assets.