U.S. DEPARTMENT OF TRANSPORTATION

OFFICE OF INSPECTOR GENERAL

FAA Has Made Progress but Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives

FAA

Report No. AV2019021

March 20, 2019

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Highlights

FAA Has Made Progress but Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives

Requested by the Committee on Transportation and Infrastructure, U.S. House of Representatives

Federal Aviation Administration | AV2019021 | March 20, 2019

What We Looked At

FAA manages air traffic control operations through a complex network of information systems and air traffic control facilities. Cyber-based threats are rapidly evolving and could threaten the connectivity of this complex aviation infrastructure. In 2016, Congress passed the FAA Extension, Safety, and Security Act. Section 2111 of the act establishes requirements for FAA to enhance cybersecurity. The Chairmen and Ranking Members of the House Committee on Transportation and Infrastructure and the Subcommittee on Aviation requested that we assess FAA's progress in addressing section 2111's requirements.

What We Found

As required by section 2111, FAA has completed a cybersecurity strategic plan, coordinated with other Federal agencies to identify cyber vulnerabilities, and developed a cyber threat model and cyber research and development plan. However, the Agency has not completed a comprehensive, strategic policy framework to identify and mitigate cybersecurity risks. For example, the Agency has not established target dates to complete implementation of recommendations from its working group established to recommend cybersecurity rulemaking and policies for aircraft systems. Furthermore, while FAA is applying its cyber threat model across the National Airspace System, mission support, and research and development areas, it has not established target dates for full model implementation. Finally, as outlined in its cybersecurity research and development plan, FAA anticipates increased investments in research areas, but has not completed decisions on its research and development priorities in upcoming fiscal years.

Our Recommendations

FAA concurred with all three of our recommendations and proposed appropriate actions and completion dates.

Contents

U.S. DEPARTMENT OF TRANSPORTATION
OFFICE OF INSPECTOR GENERAL

Memorandum

Date: March 20, 2019

Subject: INFORMATION: FAA Has Made Progress, but Additional Actions Remain To Implement Congressionally Mandated Cyber Initiatives | Report No. AV2019021

From: Matthew E. Hampton
Assistant Inspector General for Aviation Audits

To: Federal Aviation Administrator

The Federal Aviation Administration (FAA) is responsible for managing air traffic control operations in the National Airspace System (NAS) through a complex network of information systems and air traffic control facilities. FAA is currently modernizing its air traffic control operations through the implementation of the Next Generation Air Transportation System (NextGen). NextGen consists of programs, systems, and procedures that provide new capabilities, such as digital communications between controllers and pilots—known as DataComm—and other technologies including satellite-based systems for tracking and managing aircraft.

Cyber-based threats—from both internal and external sources—are rapidly evolving and could threaten the connectivity of an increasingly complex aviation infrastructure. NextGen's reliance on integrated information systems, the distribution of information, and satellite-based technologies may increase cyber-security threats to the NAS.

In 2016, Congress passed the FAA Extension, Safety, and Security Act.[1] Section 2111 of the act establishes requirements for FAA to enhance the NAS's cybersecurity. The Chairmen and Ranking Members of the House Committee on Transportation and Infrastructure and the Subcommittee on Aviation requested that we assess FAA's progress in addressing section 2111's requirements. Accordingly, our objective was to assess FAA's progress in meeting section 2111's requirements.

[1] Pub. Law No. 114-190.

We conducted this audit in accordance with generally accepted Government auditing standards. Exhibit A details our scope and methodology. Exhibit B lists the entities we visited or contacted.

We appreciate the courtesies and cooperation of Department of Transportation representatives during this audit. If you have any questions concerning this report, please call me at (202) 366-0500, or Nathan Custer, Program Director, at (202) 366-5540.

cc: The Secretary
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-100

Results in Brief

FAA has made progress meeting section 2111 requirements, but additional actions remain to implement cybersecurity initiatives across the Agency.

FAA has completed a cybersecurity strategic plan, coordinated with other Federal agencies to identify cyber vulnerabilities, developed the threat model, and established a research and development plan as required in section 2111. However, FAA has not completed a comprehensive and strategic cybersecurity framework of policies designed to identify and mitigate cybersecurity risks. Prior to passage of the act, FAA formed a joint Government-industry working group to recommend updated rulemaking and policies to enhance cybersecurity for aircraft systems. In August 2016, the group made 30 recommendations covering cybersecurity areas that FAA is considering for its framework. FAA has addressed 15 of the 30 recommendations, has 11 in progress, and has not decided whether to implement the final four. FAA officials stated that these four recommendations may not be addressed due to rulemaking priorities. FAA's lack of target dates for the four recommendations inhibits the Agency's ability to fully implement regulations and policy to mitigate cybersecurity issues for the diverse range of aircraft operating in the NAS, as required by the act. Furthermore, FAA has applied its model for identifying threats to nearly all NAS elements, including flight planning and separation assurance. The Agency is also in the early stages of applying the model to its mission support and research and development areas. However, FAA has not established target dates for risk mitigation strategies and prioritization, the final steps for fully implementing the model. FAA has yet to refine its priorities and make final decisions on additional funding for the model. As a result, it is uncertain when FAA will have threat model results to support its overall cybersecurity efforts. In addition, FAA spent $3 million in cybersecurity research in fiscal year 2018, and in its research plan anticipates increased investments over the next several years. However, it is still formulating its research and development priorities for fiscal year 2019 and beyond. A lack of prioritization of cybersecurity research and development makes it difficult for FAA to target the most needed improvements for safeguarding the NAS.

Background

FAA administers its cybersecurity efforts through its Cybersecurity Steering Committee (CSC)—established in 2014, to develop and implement an integrated cybersecurity strategy for the Agency. CSC is also responsible for preparing and delivering FAA's response to section 2111 to Congress.

To manage its air transportation infrastructure, FAA operates information systems in three areas—the NAS, the administrative network known as mission support, and research and development. FAA's Chief Information Security Officer and Chief Information Officer are responsible for cybersecurity and for ensuring that each area complies with Federal, departmental, and Agency requirements. The act requires FAA to facilitate and support the development of a comprehensive and strategic framework of principles and policies to reduce cybersecurity risks to the NAS, civil aviation, and Agency information systems using a total systems approach. A total systems approach takes into account the interactions and interdependence of aircraft system components and the NAS. Specifically, section 2111 calls for FAA to:

- develop a comprehensive and strategic framework of policies to reduce cybersecurity risks to the NAS,
- report its implementation progress to appropriate congressional committees,
- assess and research the potential cost and timetable of developing and maintaining a threat model to strengthen the cybersecurity of Agency systems and report on the development status to appropriate congressional committees,
- report on a cybersecurity standards plan to improve implementation of the National Institute of Standards and Technology's (NIST) latest revisions to information security guidance, and
- establish a cybersecurity research and development plan for the NAS.

FAA Has Made Progress Meeting Section 2111 Requirements but Additional Actions Remain

FAA has made progress meeting the requirements of section 2111, but actions to complete its cybersecurity efforts, including the cybersecurity framework,

application of its threat model to all areas, and decisions on research and development priorities remain.

FAA Has Made Progress in Meeting Section 2111 Requirements

FAA has made progress developing the cybersecurity tools that section 2111 requires, and has provided all required deliverables to the Congress. FAA is currently working on the comprehensive and strategic framework. See table 1 for details on FAA's completed efforts and progress.

Table 1. FAA's Progress in Addressing Section 2111

Section 2111 Requirement	Response/Deliverable to Congress	Due Date	Date Completed/ Submitted to Congress
Develop a comprehensive and strategic framework	No required deliverable to Congress	March 12, 2017 (240 days after enactment)	In progress
Update Congress on section 2111 implementation progress	Report	October 13, 2016 (90 days after enactment)	October 27, 2016
Assess and research cost of developing a cybersecurity threat model	Briefing	July 15, 2017 (365 days after enactment)	August 31, 2017
Transmit a plan for cybersecurity standards based on NIST guidelines	Report	January 11, 2017 (180 days after enactment)	June 19, 2017
Establish a cybersecurity research and development plan	No required deliverable to Congress	July 15, 2017 (365 days after enactment)	July 11, 2017

Source: OIG analysis

FAA Is Developing Its Comprehensive and Strategic Cybersecurity Framework but its Implementation Lacks Some Target Dates

FAA is developing a comprehensive and strategic cybersecurity framework as required by section 2111. A comprehensive framework includes cybersecurity principles and policies designed to identify and address cybersecurity risks throughout the agency. FAA's framework currently includes a strategic plan for cybersecurity that articulates the Agency's strategy for protecting FAA's information systems and mission. The strategic plan, which is updated annually, defines a set of strategic goals and supporting objectives that guide FAA's Agency-wide approach to cybersecurity.

The framework's development requires FAA to coordinate with other Federal agencies and stakeholders. With the Departments of Defense and Homeland Security (DHS), FAA participates in the Aviation Cybersecurity Initiative—an interagency task force.[2] The task force's draft charter[3] will establish a tri-chair among the three agencies. The Initiative's objective is to identify and mitigate cyber vulnerabilities in the "Aviation Ecosystem," which includes airline and airport systems and other aspects of the aviation industry.

The framework also requires that FAA identify and address cybersecurity risks associated with aircraft systems. Prior to the passage of the act, in December 2014, FAA created a joint Government-industry working group—the Aircraft Systems Information Security Protection working group (Working Group)—to leverage industry expertise for the enhancement of cybersecurity for aircraft systems.[4] FAA has tasked the Working Group to do several things, including provide recommendations regarding rulemaking, policy, and guidance to enhance cybersecurity. Furthermore, the act directs the Working Group to (1) assess cybersecurity risks to aircraft systems, (2) review the extent to which existing rulemaking and policy promote aircraft systems information security protection, and (3) provide recommendations if additional rulemaking and policies are needed to address cybersecurity risks to aircraft systems.

In its report[5] submitted to FAA in August 2016, the Working Group made 30 recommendations that cover several areas of cybersecurity[6] that FAA is considering for the development of its comprehensive and strategic framework. FAA's Office of Aviation Safety (AVS) is responsible for implementing the Working Group's recommendations. As of August 2018, AVS had completed or closed 15 recommendations. It had completed certain recommendations with updates to rules or regulations associated with the recommendation, and closed others with verification that past actions were sufficient or that further actions were not needed. For example, one completed recommendation updated cybersecurity

[2] The Federal Bureau of Investigation and the Office of the Director of National Intelligence are also initiative members.

[3] The Aviation Cybersecurity Initiative charter is being revised to conform to DHS's National Strategy for Aviation Security and is being reviewed on the department level by each of the three agencies.

[4] The Working Group includes members and subject matter experts from industry and government including airframe and avionics manufacturers, industry standards groups, operators, regulators and other aviation stakeholders.

[5] *A Report from the Aviation Rulemaking Advisory Committee Aircraft System Information Security/Protection Working Group to the Federal Aviation Administration*, August 22, 2016.

[6] These areas include cybersecurity for large transport aircraft, general aviation, rotorcraft, avionics, and other aviation equipment.

policies for "special conditions"—a type of regulation that applies to a particular aircraft design.[7] For a complete list of the 30 recommendations, see exhibit D.

During our review, AVS was completing implementation of 11 recommendations. It has established target dates from 2018 to 2020 for these recommendations. For example, one recommendation calls for FAA to develop guidance on security protection for aircraft-installed equipment intended to connect to portable electronic devices such as electronic flight bags by May 2019.

AVS has deferred actions on four recommendations—covering engines, propellers, rotorcraft, and general aviation aircraft—that are dependent on the completion of related activities or associated risk evaluations. FAA has not decided whether it will establish target dates for these deferred recommendations. AVS officials informed us that these four recommendations may not be addressed because of rulemaking and resource priorities.

Target dates provide useful information for stakeholders and promote timely completion. FAA's lack of target dates for the deferred recommendations inhibits the Agency's ability to fully implement regulations and policy to mitigate cybersecurity issues for a diverse range of aircraft operating in the NAS, as required by the act.

FAA Has Yet To Complete Threat Model Applications and Set Research and Development Priorities

FAA has not established timeframes for the full application of the threat model to each of its operation areas or set priorities for research and development initiatives.

FAA Has Not Yet Completed the Application of the Threat Model Across Its Three Operation Areas

In August 2017, FAA briefed Congress on the status of its development of a cybersecurity threat model. The model—referred to as the Cybersecurity Risk Model (CyRM) and developed in conjunction with the MITRE Corp.—is designed to identify and assess risk for FAA systems by taking an end-to-end approach to assess cybersecurity threats. In this approach, CyRM analyzes data exchanges

[7] FAA issues special conditions when it finds that airworthiness regulations for an aircraft, aircraft engine, or propeller design do not contain adequate or appropriate safety standards because of a novel or unusual design feature.

across rather than within systems. CyRM's risk assessment process includes threat identification and identification of mitigation methods.

FAA has applied the model to identify threats and assess risk for seven of the nine NAS service elements with plans to complete all nine by December 2018. Completed service elements include flight planning and separation assurance—keeping aircraft safely apart in all phases of flight. The Agency is also in the early stages of applying the model to its mission support and research and development areas. However, it has not established target dates for threat mitigation strategies and risk prioritization, the final steps for fully implementing the model. FAA is still developing priorities for CyRM, and its future CyRM efforts—such as identifying new threats—will involve final decisions on additional funding. Consequently, it is uncertain when FAA will have complete threat model results to support its cybersecurity efforts and whether it will undertake further model applications.

FAA Has Not Decided on Its Cybersecurity Research and Development Priorities

In July 2017, FAA established its cybersecurity research and development plan, as required by section 2111. This plan represents a baseline that FAA will update to reflect coordination with other Federal aviation research and development. The current plan's research areas and specific tasks include, among other things, assessment and analysis of connectivity to aircraft systems to identify vulnerabilities and risks that impact aircraft safety, including evaluation of cybersecurity risks in passenger cabin communications—specifically outlined in section 2111. The current plan also outlines a proposal for cooperation with international partners and other Federal agencies and steps the Agency is taking to coordinate with those agencies, including on cybersecurity testing of commercial aircraft.[8]

In the plan, FAA has established broad objectives, milestones, outcomes, and 5-year funding profiles for specific research and development efforts through 2022. See exhibit E for details on the cybersecurity research areas. FAA spent $3 million in fiscal year 2018 on cybersecurity research and development, and, according to the plan, anticipates significant increases in these investments over the next several years. However, FAA is still formulating its research and development requirements and priorities for fiscal year 2019 and beyond. This lack of finalized priorities makes it difficult for FAA to pursue improved safeguards for the NAS and limits the Agency's ability to achieve a total systems cybersecurity approach.

[8] FAA and DHS are working with the Boeing Company to assess cybersecurity aspects of Boeing's 757 aircraft at FAA's William J. Hughes Technical Center in New Jersey.

Conclusion

The sophistication of cyber threats continues to increase and evolve. FAA's development of the cybersecurity tools to meet requirements under section 2111 is a significant step in the enhancement of the Agency's cybersecurity to stay abreast of the rapid development of these threats. However, implementation delays of cybersecurity tools inhibit FAA's ability to keep its cybersecurity up-to-date and make it difficult for the Agency to fully identify and mitigate vulnerabilities.

Recommendations

To improve FAA's ability to implement its cybersecurity requirements in accordance with section 2111, we recommend that the Federal Aviation Administrator:

1. Develop a plan with target dates to address the Working Group's four deferred recommendations to enhance aircraft systems cybersecurity.

2. Develop a plan with target dates to finalize the application of CyRM to the mission support and research and development areas, and determine when full application of CyRM will occur.

3. Establish priorities for FAA-led research and development activities and incorporate these priorities into the budget process.

Agency Comments and Office of Inspector General Response

We provided FAA with our draft report on November 14, 2018, and received its formal management response on December 11, 2018, which is included as an appendix to this report. FAA also provided technical comments which we incorporated into this report where appropriate. In its management response, FAA concurred with all three of our recommendations and proposed appropriate actions and completion dates. Accordingly, we consider all recommendations as resolved but open pending completion of the planned actions.

Exhibit A. Scope and Methodology

We conducted this performance audit between August 2017 and November 2018 in accordance with generally accepted Government auditing standards as prescribed by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The House Committee on Transportation and Infrastructure and its Aviation Subcommittee directed our office to provide an update on FAA's progress in addressing components of Section 2111 of the FAA Extension, Safety, and Security Act of 2016. Accordingly, our audit objective is to assess FAA's progress in meeting the requirements of Section 2111 of the FAA Extension, Safety, and Security Act of 2016.

We collected and analyzed documentation from FAA on cybersecurity and actions taken to satisfy the act's requirements. These documents include the reports and briefings FAA provided to Congress in response to the legislation, a report by the Working Group sponsored by the Aviation Rulemaking Advisory Committee, the latest guidance from the NIST on information security, FAA Business Plans, and FAA's cybersecurity research and development plan.

We interviewed pertinent representatives of FAA's CSC including FAA's Air Traffic Organization, Aviation Safety, Office of NextGen, Office of Finance and Management; and the DOT Office of the Chief Information Security Officer. We also interviewed associated FAA offices such as the Aviation Research Division and Office of Management Services. We also met with cybersecurity officials from the MITRE Corporation and the Boeing Aircraft Company.

Exhibit B. Organizations Visited or Contacted

Federal Aviation Administration Headquarters

Air Traffic Organization

- NAS Security and Enterprise Operations

Aviation Safety

- Policy and Innovation Division

Office of NextGen

- NAS Systems Engineering and Integration Office
- Aviation Research Division (Atlantic City, NJ)
- Office of Management Services

Office of Finance and Management

- Office of Information Security and Privacy

Department of Transportation Headquarters

Office of the Chief Information Security Officer

Other Organizations

Boeing Aircraft Company (Washington, DC)

MITRE Corporation, (McLean, VA)

Exhibit C. List of Acronyms

AVS	Office of Aviation Safety
CSC	Cybersecurity Steering Committee
CyRM	Cybersecurity Risk Model
DHS	U.S. Department of Homeland Security
DOT	U.S. Department of Transportation
FAA	Federal Aviation Administration
NAS	National Airspace System
NextGen	Next Generation Air Transportation System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

Exhibit D. Status of the Working Group's 30 Recommendations

No.	Completed/Closed Recommendations by FAA
1	**Recommendation 01:** Work closely with primary certification authorities to harmonize airworthiness standards and guidance for aircraft system information security/protection.
2	**Recommendation 04:** Establish guidance for minor or lower equipment that has connectivity with other systems which should be protected.
3	**Recommendation 05:** Create harmonized standards around the risk acceptability and assurance framework. This harmonized standards material should be incorporated into the appropriate domestic and European documents.
4	**Recommendation 07:** Create listing for regulation which scoped editing of documents to several technical working group recommendations.
5	**Recommendation 08:** Work on guidance materials topics 1-9.
6	**Recommendation 11:** The Working Group notes that domestic and European are currently not aligned with respect to their applicability to rotorcraft and recommends that the documents should be updated and tailored to better address rotorcraft.
7	**Recommendation 16:** Encourages the in-flight entertainment (IFE) systems and connectivity industry to participate in information sharing partnerships.
8	**Recommendation 17:** Set a legal basis for prohibiting tampering with aircraft systems.
9	**Recommendation 18:** Not to establish additional security requirements for IFE systems–because additional regulatory requirements for IFE software could negatively affect the security posture when IFE software has to be upgraded.
10	**Recommendation 19:** Existing policies for type design changes, such as the establishment of certification basis, for existing safety regulations and means of compliance are also applicable to Working Group considerations and a phased adoption of industry standards should be anticipated.
11	**Recommendation 20:** Update the policy statement for the establishment of special conditions for cyber security based on the input provided by the Working Group.
12	**Recommendation 21:** Establish policy to leverage existing Continued Operational Safety programs for reporting security events affecting safety.
13	**Recommendation 22:** Update domestic and European standards to include guidance for logging for large transport category airplanes**.**
14	**Recommendation 27:** Review the existing communications, navigation, and surveillance (CNS) technical standards orders in coordination with industry and determine if targeted risk mitigations should be integrated into future revisions to specific standards. Some of this work is already underway,

No.	Completed/Closed Recommendations by FAA
	but a comprehensive table top review of the CNS avionics standards would help to mitigate risk and address concerns.
15	**Recommendation 28:** Have the Aviation Information Sharing and Analysis Center and the U.S. Computer Emergency Readiness Team should continue to develop capabilities to address aviation system specific threats and issues in support of ensuring a safe and secure aviation industry.

No.	In Progress Recommendations by FAA
1	**Recommendation 02:** Undertake rulemaking to update standards for transport category airplanes.
2	**Recommendation 03:** Consider domestic and European standards acceptable guidance material to comply with transport category airplane security rules.
3	**Recommendation 06:** Establish guidance to show compliance with the rule requiring an applicant to define a security environment as required input of any security analysis.
4	**Recommendation 09:** Consider the results of the RTCA, Inc. information security committee tasking as part of the agency's development of guidance for the listed in the Working Group report.
5	**Recommendation 13:** Support industry development of best practices for small airplane standards.
6	**Recommendation 23:** Encourage adoption of general aviation and international standard security best practices for logging considerations.
7	**Recommendation 24:** Develop guidance to address security protection on aircraft installed equipment intended to connect to portable electronic devices (PEDs).
8	**Recommendation 25:** Establish guidance for field loadable software including aircraft databases.
9	**Recommendation 26:** Establish guidance for the use of commercial off the shelf and previously certified products.
10	**Recommendation 29:** Develop and provide clear standards for security designations for designees.
11	**Recommendation Research R1:** Consider the following topics as part of future agency research to address cybersecurity: - determine how threat and vulnerability sharing can be most effectively done for the Working Group including in coordination with international partners and regulators. - development of tools that can facilitate event log analysis. - detecting and preventing vulnerabilities from PED's connectivity to avionic interface devices. - detecting vulnerabilities in receiving transponder and Automatic Dependent Surveillance - Broadcast data in aircraft.

No.	Deferred Recommendations by FAA
1	**Recommendation 10:** Undertake rulemaking to update standards for normal and transport category rotorcraft.
2	**Recommendation 12:** Base aviation system related small airplane guidance on "abnormal operation" of the small airplane rule.
3	**Recommendation 14:** Undertake rulemaking to update standards to provide security protection for engines.
4	**Recommendation 15:** Undertake rulemaking to update standards to establish information security protection for propellers.

Source: FAA

Exhibit E. Cybersecurity Research and Development Areas and Cost Estimates[a] (dollars in thousands)

Research Area	Requirement	2018 Requested	2019 Estimate	2020 Estimate	2021 Estimate	2022 Estimate
Security and Resiliency (methods to enhance the ability to prevent, detect, and respond to cyber-attacks)	Aviation Systems	$2,000	[redacted]	[redacted]	[redacted]	[redacted]
	Cybersecurity risks of cabin communications and systems	$0	[redacted]	[redacted]	[redacted]	[redacted]
	Unmanned aircraft system networked link	$310	[redacted]	[redacted]	[redacted]	[redacted]
Data Analytics (analytical capabilities for aggregating data to predict and respond to cyber-attacks)	Flight deck data exchange	$0	[redacted]	[redacted]	[redacted]	[redacted]
	NextGen-information security	$1,000	[redacted]	[redacted]	[redacted]	[redacted]
	Identity and authorization management interoperability	$0	[redacted]	[redacted]	[redacted]	[redacted]
Human Behavior/Human Factors (human-in-the-loop policies, training, and procedures to detect and respond to cyber-attacks)	Aviation systems response and recovery	$0	[redacted]	[redacted]	[redacted]	[redacted]
	Situational awareness, visualization, threat assessment, and compliance	$0	[redacted]	[redacted]	[redacted]	[redacted]
System Wide Safety Assurance (real time, continuous, safety analysis and assurance tools to mitigate the impact of cyber-attacks)	Unmanned aircraft system security control capability	$400	[redacted]	[redacted]	[redacted]	[redacted]
	Cybersecurity test facility virtualization	$0	[redacted]	[redacted]	[redacted]	[redacted]
Total		$3,710	[redacted]	[redacted]	[redacted]	[redacted]

[a] These cost estimates are from FAA's cybersecurity research and development plan. We have redacted the estimates from 2019 to 2022 because DOT made a determination that the estimates for future years are not available for public release at this time.
Source: FAA

Exhibit F. Major Contributors to This Report

NATHAN **CUSTER**	PROGRAM DIRECTOR
ARNETT **SANDERS**	PROJECT MANAGER
WON **KIM**	SENIOR AUDITOR
KIESHA **MCMILLAN**	SENIOR AUDITOR
MI HWA **BUTTON**	ANALYST
TAMARIA **KELLY**	ANALYST
SUSAN **NEILL**	WRITER-EDITOR
AMY **BERKS**	SENIOR COUNSEL

Appendix. Agency Comments

Federal Aviation Administration

Memorandum

Date: December 11, 2018

To: Matthew E. Hampton, Assistant Inspector General for Aviation Audits

From: H. Clayton Foushee, Director, Office of Audit and Evaluation, AAE-1

Subject: Federal Aviation Administration's (FAA) Response to Office of Inspector General (OIG) Draft Report: FAA's Implementation of Congressionally Mandated Cyber Initiatives

Aircraft and air traffic control operations are increasingly reliant upon cyber networks, and the security of these systems is a worldwide priority. Section 2111 of the FAA Extension, Safety, and Security Act of 2016 mandated a number of cyber security requirements aimed at the protection of FAA systems and partnership with the private sector to address cyber security risks to the global aviation system. OIG recognized our cyber security accomplishments in its draft report by stating, "FAA has made progress developing the cyber security tools that Section 2111 requires, and has provided all required deliverables to the Congress."

FAA's recent cyber security accomplishments include the following:

- Developed the Aircraft Systems Information Security Protection (ASISP) Plan with detailed initiatives designed to address safety risks associated with information security for avionic systems, including associated networks. The plan focuses on initiatives to address 30 recommendations made by the Aviation Rulemaking Advisory Committee (ARAC) ASISP Working Group.
- Developed FAA's Cyber Security Strategy which articulates goals and objectives, and are aligned to specific projects with milestones for completion.
- Completed the Cyber Security Test Facility (CyTF) at the William J. Hughes Technical Center. The CyTF provides the FAA with new tools to identify cyber security vulnerabilities and risks through the conduct of frequent cyber security exercises and evaluations.
- Updated the Cyber Research and Development Plan prioritized cyber security

activities based upon risk identification and mission requirements.

- Developed a Cyber Security Risk Model (CyRM) plan and a CyRM methodology manual. These documents outline a common foundation and structure for an effective and integrated agency-wide CyRM.2

Upon review of the draft report, we concur with recommendations 1, 2, and 3. With regard to recommendation 1, we plan to update the ASISP Plan by September 30, 2019 to reflect new target dates for the recommendations. For recommendation 2, FAA plans to update the CyRM strategy and plan by September 30, 2019 to include target dates for the full implementation of CyRM. FAA concurs with recommendation 3 and plans to complete actions by September 30, 2019.

We appreciate the opportunity to respond to the OIG draft report. Please contact H. Clayton Foushee at (202) 267-9000 if you have any questions or require additional information about these comments.

U.S. DOT OIG

Fraud & Safety Hotline

hotline@oig.dot.gov | (800) 424-9071

https://www.oig.dot.gov/hotline

Our Mission

OIG conducts audits and investigations on behalf of the American public to improve the performance and integrity of DOT's programs to ensure a safe, efficient, and effective national transportation system.

OFFICE OF INSPECTOR GENERAL
U.S. Department of Transportation
1200 New Jersey Ave SE
Washington, DC 20590

www.oig.dot.gov