U.S. Department
of Transportation
**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., SW.
Washington, DC 20591

August 14, 2020

The Honorable Roger Wicker
Chairman, Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC 20510

Dear Chairman Wicker:

As required by Section 509(d) of the FAA Reauthorization Act of 2018, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to initiate a review of the comprehensive and strategic framework of principles and policies developed pursuant to Section 2111 of the FAA Extension, Safety, and Security Act of 2016. In undertaking the review, the FAA was required to:

(1) Assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system;

(2) Review existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system; and

(3) Assess the Administration's level of engagement and coordination with aviation stakeholders and other appropriate agencies, organizations, or groups with which the Administration consults to carry out the framework.

The enclosed report describes the results of the review and modifications made to the FAA Cybersecurity Strategy. We have sent identical letters to Chairman DeFazio, Senator Cantwell, and Congressman Graves.

If I can be of further assistance, please contact me or the Office of Government and Industry Affairs at (202) 267-3277.

Sincerely,

Steve Dickson
Administrator

Enclosure

U.S. Department of Transportation
Federal Aviation Administration

Office of the Administrator

800 Independence Ave., SW.
Washington, DC 20591

August 14, 2020

The Honorable Maria Cantwell
Committee on Commerce, Science, and Transportation
United States Senate
Washington, DC 20510

Dear Senator Cantwell:

As required by Section 509(d) of the FAA Reauthorization Act of 2018, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to initiate a review of the comprehensive and strategic framework of principles and policies developed pursuant to Section 2111 of the FAA Extension, Safety, and Security Act of 2016. In undertaking the review, the FAA was required to:

(1) Assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system;

(2) Review existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system; and

(3) Assess the Administration's level of engagement and coordination with aviation stakeholders and other appropriate agencies, organizations, or groups with which the Administration consults to carry out the framework.

The enclosed report describes the results of the review and modifications made to the FAA Cybersecurity Strategy. We have sent identical letters to Chairman DeFazio, Chairman Wicker, and Congressman Graves.

If I can be of further assistance, please contact me or the Office of Government and Industry Affairs at (202) 267-3277.

Sincerely,

Steve Dickson
Administrator

Enclosure

U.S. Department
of Transportation
**Federal Aviation
Administration**

Office of the Administrator

800 Independence Ave., SW.
Washington, DC 20591

August 14, 2020

The Honorable Peter A. DeFazio
Chairman, Committee on Transportation and Infrastructure
House of Representatives
Washington, DC 20515

Dear Chairman DeFazio:

As required by Section 509(d) of the FAA Reauthorization Act of 2018, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to initiate a review of the comprehensive and strategic framework of principles and policies developed pursuant to Section 2111 of the FAA Extension, Safety, and Security Act of 2016. In undertaking the review, the FAA was required to:

(1) Assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system;

(2) Review existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system; and

(3) Assess the Administration's level of engagement and coordination with aviation stakeholders and other appropriate agencies, organizations, or groups with which the Administration consults to carry out the framework.

The enclosed report describes the results of the review and modifications made to the FAA Cybersecurity Strategy. We have sent identical letters to Chairman Wicker, Senator Cantwell, and Congressman Graves.

If I can be of further assistance, please contact me or the Office of Government and Industry Affairs at (202) 267-3277.

Sincerely,

Steve Dickson
Administrator

Enclosure

U.S. Department of Transportation
Federal Aviation Administration

Office of the Administrator

800 Independence Ave., SW.
Washington, DC 20591

August 14, 2020

The Honorable Sam Graves
Committee on Transportation and Infrastructure
House of Representatives
Washington, DC 20515

Dear Congressman Graves:

As required by Section 509(d) of the FAA Reauthorization Act of 2018, the Federal Aviation Administration (FAA) is pleased to provide the enclosed report.

The Act requires the FAA to initiate a review of the comprehensive and strategic framework of principles and policies developed pursuant to Section 2111 of the FAA Extension, Safety, and Security Act of 2016. In undertaking the review, the FAA was required to:

(1) Assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system;

(2) Review existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system; and

(3) Assess the Administration's level of engagement and coordination with aviation stakeholders and other appropriate agencies, organizations, or groups with which the Administration consults to carry out the framework.

The enclosed report describes the results of the review and modifications made to the FAA Cybersecurity Strategy. We have sent identical letters to Chairman DeFazio, Chairman Wicker, and Senator Cantwell.

If I can be of further assistance, please contact me or the Office of Government and Industry Affairs at (202) 267-3277.

Sincerely,

Steve Dickson
Administrator

Enclosure

Section 509 of the FAA Reauthorization Act of 2018 Report to Congress

Summary

In accordance with Section 509 of the FAA Reauthorization Act of 2018, the Federal Aviation Administration (FAA) initiated a review of the comprehensive and strategic framework of principles and policies (hereinafter, the ‘‘framework’’) developed pursuant to Section 2111 of the FAA Extension, Safety, and Security Act of 2016. This report summarizes the outcome of our review and accomplishments that continue to strengthen the cybersecurity posture of the aviation ecosystem.

The framework consists of five pillars: 1) refine and maintain a cybersecurity governance structure to enhance cross-domain synergy; 2) protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery; 3) enhance data-driven risk management decision capabilities; 4) build and maintain workforce capabilities for cybersecurity; and 5) build and maintain relationships with, and provide guidance to, external partners in government and industry to sustain and improve cybersecurity in the aviation ecosystem. This framework of five pillars is the foundation of the FAA's Cybersecurity Strategy, and drives FAA's progress on initiatives supporting each of those pillars.

The FAA continues to maintain and enhance a strong cybersecurity governance process, creating a strong synergy between the three domains of the FAA – National Airspace System (NAS), Research and Development (R&D), and Mission Support (MS). This is accomplished with the collaboration of the Office of Finance & Management (AFN), Air Traffic Organization (ATO), NextGen (ANG), Aviation Safety (AVS), the Office of Airports (ARP), and the Office of Security & Hazardous Materials Safety (ASH), as members of the FAA Cybersecurity Steering Committee (CSC). With the input of these groups, other FAA offices as needed, and oversight of the CSC, the FAA continues to review, update, and maintain the framework to support a more cyber secure and resilient aviation ecosystem.

The 2019 annual review resulted in updates to the FAA Cybersecurity Strategy to ensure alignment with the National Cybersecurity Strategy and National Strategy for Aviation Security. In addition, enhancements were made to address the growing use of cloud and "as-a-service" technologies. The Strategy was also modified to reflect efforts to improve response times in mitigation of internet-facing vulnerabilities, as well as solid cyber hygiene principles. Lastly, the Strategy was strengthened by including a focus on external stakeholder engagement activities to include information-sharing and best practices around aviation cybersecurity.

The FAA CSC determined through its review that there were no deficiencies in the framework and thus no significant changes were required. Accordingly, FAA focused on updating the FAA's Cybersecurity Strategy to reflect advancements. Included in this report are accomplishments of note that will continue to improve our cybersecurity posture, and that of the aviation ecosystem.

Introduction

In 2015, the FAA created the first five-year FAA Cybersecurity Strategy, which articulated the Agency's strategy for protecting FAA information systems, and the FAA mission they support, from cybersecurity threats. The purpose of this Strategy was, and still is, to guide the development of the FAA cybersecurity program and strengthen the overall FAA cybersecurity posture. Additionally, the Strategy articulates FAA engagement with public and private sector partners to address cybersecurity risk across the aviation ecosystem. The FAA Cybersecurity Strategy, updated annually, sets clear goals and objectives for the FAA's cybersecurity program to safeguard the Agency's information assets and assure the confidentiality, integrity, and availability of the information vital to achieve its missions. The FAA Cybersecurity Strategy 2020-2025 represents the FY 2019 update and will guide cybersecurity at the FAA for the next five years. The FAA will implement this Strategy through active engagement and support from all stakeholders.

Review of FAA Strategic Cybersecurity Plan

In 2019, the FAA undertook its review of the framework and the associated Strategy through the CSC working group, which is composed of representatives from the FAA organizations that are represented on the CSC. The CSC working group members bring subject matter expertise in cybersecurity within each of their respective aviation areas and work with their respective stakeholders for additional review and input to the Strategy.

The review focused on examining the following:

(1) Assess the degree to which the framework identifies and addresses known cybersecurity risks associated with the aviation system

The CSC working group assessed the framework and reviewed the Strategy with respect to its suitability for the current aviation cybersecurity environment, as well as cybersecurity threats and vulnerabilities that may affect the FAA's enterprise IT environments. Overall, the CSC working group determined that the framework was sound and the content of the Strategy articulated goals and objectives that address known cybersecurity risks in the aviation system, also referred to as the aviation ecosystem. The Strategy articulates these themes and the CSC

working group determined that this reflects the foundation of a successful cybersecurity program to address current risks, while possessing the necessary agility to adapt to future risks.

(2) Review existing short- and long-term objectives for addressing cybersecurity risks to the national airspace system

The CSC working group considered the potential impacts of new technologies in the National Airspace System (NAS), as well as the long operational lifespan of aviation systems, to ensure the Strategy encompassed evolving advancements in technology, such as cloud and service-delivered capabilities, as drivers for the strategic goals. The CSC working group validated that the Cybersecurity Test Facility (CyTF) continues to be a key element for evaluating cybersecurity risks. Enterprise threat modeling is a long-term objective to provide a structured approach in addressing risks and developing plans to mitigate those risks in the NAS. Information Security Continuous Monitoring (ISCM) is also a long-term objective to establish and maintain ongoing awareness of organizational security posture, vulnerabilities and threats to support risk management decisions. Vulnerability mitigation continues as both a short-term tactical objective and long-term component of improved system hygiene.

(3) Assess the FAA's level of engagement and coordination with aviation stakeholders and other appropriate agencies, organizations, or groups with which the FAA consults to carry out the framework.

Cybersecurity is a growing focus within the aviation ecosystem and of stakeholders across industry and government, as well as international bodies, civil aviation authorities, and air navigation service providers. The CSC working group considered this in addition to the increasing volume of requests for FAA engagement in cybersecurity efforts at both the inter-agency and international levels. FAA engagement with industry groups includes the Aircraft Systems Information Security Protection (ASISP) working group, Aviation Sector Coordinating Council (ASCC), and the Aviation Information Sharing and Analysis Center (ISAC). Inter-agency engagement includes the Aviation Government Coordinating Council (AGCC) and both inter-agency and industry engagement as a Tri-Chair of the Aviation Cyber Initiative (ACI). The CSC determined collectively that this diverse set of engagement paths reflects a suitable foundation of engagement and coordination. This is further augmented by FAA's continuous engagement in inter-agency cyber exercises with participation from both domestic and international government and non-government stakeholders. The FAA is also actively involved in and leading many International Civil Aviation Organization (ICAO) efforts to develop global approaches to aviation cybersecurity, and enable cybersecurity and resiliency in the global aviation ecosystem. The FAA will continue to build relationships with external partners in government and industry in support of information-sharing to sustain and improve cybersecurity in the aviation ecosystem. These efforts are in addition to any regulatory approaches deemed necessary to maintain a safe, secure, and efficient aviation ecosystem.

Results of Review and Accomplishments

The FAA Cybersecurity Steering Committee focuses on the FAA's cybersecurity needs and priorities in order to effect an integrated approach to the protection of FAA systems, networks, and information that collectively support the FAA. In particular, the CSC identifies and agrees upon the cybersecurity priorities, strategies, and operational guidelines in support of an integrated Agency-wide approach to protecting the FAA from cybersecurity threats. Through regular meetings, the CSC works across the FAA to ensure consistent risk acceptance decisions, coordinates FAA-wide cybersecurity-related activities, and monitors cybersecurity resources to ensure they are properly allocated for efficiency and to minimize redundancy. The CSC also responds to urgent matters through ad hoc CSC discussions to provide timely direction regarding critical needs. Additionally, the CSC has and will create working groups, as needed, to address specific threats, or longer term efforts requiring dedicated planning and resources.

With regard to the FAA's Strategy, the CSC continuously reviews and updates it to ensure alignment with the evolving cybersecurity threat landscape and promote a cyber-secure and resilient aviation ecosystem. This mature and robust process ensures a relevant Strategy that focuses the Committee's engagement efforts on enhancing FAA's cybersecurity posture, as well as strengthening the cybersecurity of the aviation ecosystem as a whole.

The FAA continues a robust engagement with industry to identify and address cybersecurity-related safety risks in aircraft systems. Specifically, the FAA continues to make progress with the implementation of recommendations from the Aviation Rulemaking Advisory Committee (ARAC) working group for Aircraft Systems Information Security Protection (ASISP). These recommendations address aircraft cybersecurity protections through industry consensus standards, as well as regulations. Of the 30 recommendations provided by the working group, over half have been completed and the remainder are being actively worked, including through an update to transport airplane regulations via the rulemaking processes.

Also, in 2019, the FAA undertook and completed an update to its overarching information security and privacy policy. FAA Order 1370.121A "FAA Information Security and Privacy Program & Policy" is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Security and Privacy Controls for Information Systems and Organizations, Presidential Directives, Executive Orders, OMB Memorandums, Department of Defense (DOD) requirements (as appropriate), Department of Homeland Security (DHS) Binding Operational Directives (BOD), the Federal Risk and Authorization Management Program (FedRAMP), the Privacy Act, the Department of Transportation's (DOT) Cybersecurity Compendium, and other Federal policies and guidance. As part of the FAA's review and update of this policy, it was significantly enhanced to address the use of emerging technologies (e.g., cloud), while ensuring safe and secure integration into the FAA environment. Additionally, enhanced policy was needed to counteract or reduce the impact of new and more aggressive

cybersecurity threats. Furthermore, the update provides alignment with new Federal policies, directives, orders, and guidance that levied new cybersecurity requirements for the protection of agency information technology systems, information and data, and personnel.

With growing concern and focus on supply chain, the FAA has recognized the importance of protecting the entire supply chain. The FAA is addressing this through ongoing efforts to ensure the FAA acquisition management process includes cybersecurity and privacy clauses. The FAA, under the auspices of the CSC, continues to review Acquisition Management System (AMS) clauses in the context of cybersecurity and supply chain risks to identify any new updates that may be needed.

The FAA also made significant progress toward the implementation of Continuous Diagnostics & Mitigation (CDM) capabilities, the Cyber Risk Model (CyRM), and enhanced cybersecurity training and awareness. The Cyber Test Facility (CyTF) continues to expand and improve its capacity for simulation of FAA systems, including air traffic control components, as well as capabilities for supporting classified activities. The FAA focused on enhancing the enterprise security architecture, tooling inventory, and overall research and development (R&D) plan to ensure cybersecurity remained a predominant theme throughout.

In 2019, the FAA completed a comprehensive review of its Security Operations Center (SOC) tool suite, and made changes, as appropriate, to assure that FAA SOC threat intelligence, incident response, and hunting capabilities continue to align with industry best practices.

The FAA, in coordination with the other Tri-Chair Departments, finalized the ACI Charter with resultant signatures by the Secretaries of Defense, Homeland Security, and Transportation. The ACI established its Executive Committee, consisting of Assistant Director/Deputy Assistant Secretary/Deputy Administrator level representatives from the three Tri-Chair Departments. ACI is currently working collaboratively on an effort to examine and develop solutions for cybersecurity concerns around transponder vulnerabilities, which is expected to have direct positive mission impact for both DOD and FAA. Additionally, ACI has been engaged with aviation ecosystem stakeholders through the ACI Community of Interest, which facilitates information sharing among over 250 participants from the public and private sectors. Internationally, FAA is leading and participating in an increasing volume of cyber-focused engagements related to aviation, including information sharing round tables, training exercises, and participation in aviation cyber-focused conferences. These international engagements are being accomplished both directly by the FAA and through the ACI.

Finally, the FAA has continued to actively engage with numerous external partners from other Federal Departments and Agencies, as well as international partners and private industry. The FAA is an active participant in International Civil Aviation Organization (ICAO) groups focused on cybersecurity, including leading a group developing a global trust framework for

communications across the global aviation ecosystem, as well as efforts to raise the prominence of, and improve the governance structure for, cybersecurity at ICAO. The FAA has engaged with international partners, and continues to do so, for both cybersecurity exercises and information sharing on best practices for aviation cybersecurity. The FAA is continuing engagement on cybersecurity information sharing with the Aviation Information Sharing and Analysis Center, a private industry information security group; DHS, through the National Cybersecurity and Communications Integration Center; and partners in the Intelligence Community.