STATEMENT OF
LARRY GROSSMAN, CHIEF INFORMATION SECURITY OFFICER
FEDERAL AVIATION ADMINISTRATION

HEARING BEFORE THE UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON TRANSPORTATION AND INFRASTRUCTURE:
THE EVOLVING CYBERSECURITY LANDSCAPE: FEDERAL PERSPECTIVES ON SECURING THE NATION'S INFRASTRUCTURE

December 2, 2021

Good morning Chair DeFazio, Ranking Member Graves, and Members of the Committee:

Thank you for the opportunity to be here with you today to discuss the Federal Aviation Administration's (FAA) approach to cybersecurity, both in terms of how the FAA addresses cybersecurity matters internally and how the FAA interacts with the aviation community on cybersecurity matters.

The core and continuing mission of the FAA is to provide the safest and most efficient aerospace system in the world. Technology has contributed greatly to the safety and efficiency of the national airspace system (NAS). It has also resulted in highly integrated and increasingly interdependent computers and networks supporting the aviation community. Cyber-based threats have made the integration of cybersecurity protections into all aspects of the FAA's mission increasingly important. This Administration has recognized the growing importance of cybersecurity. President Biden's Executive Order 14028, "Improving the Nation's Cybersecurity", is a sweeping directive that addresses cyber threat information sharing, cybersecurity modernization, software supply chain security, identifying and remediating cyber vulnerabilities, and incident response.[1] This executive order will drive many elements of FAA's

[1] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

strategic cyber initiatives across both the agency's IT infrastructure as well as the infrastructure of the NAS.

FAA's Cybersecurity Structure and Strategy

To achieve its mission, the FAA is dependent on information systems, and operates these systems in three separate domains: the NAS Domain, operated by FAA's Air Traffic Organization (ATO), the Mission Support Domain, operated by FAA's Office of Finance and Management (AFN), and the Research and Development Domain, operated by FAA's Office of NextGen (ANG). Each of the three domains represents a separate security perimeter with a distinct set of security controls. While each FAA Domain operator is responsible for the cybersecurity of its infrastructure, the FAA Chief Information Security Officer (CISO) and the Chief Information Officer have overall responsibility for the FAA's cybersecurity and ensuring that Domain operators comply with applicable agency, departmental, and federal requirements.

Overall, the FAA manages all aspects of the agency's cybersecurity mission through the Cybersecurity Steering Committee (CSC). The CSC was established in 2014 after the agency recognized the need to work more holistically at cybersecurity across the FAA enterprise. The CSC is charged with developing the FAA's cybersecurity strategy, setting priorities, and operational guidelines in support of an integrated agency-wide approach to protecting the FAA from cyber-threats. The FAA Cybersecurity Strategy was first developed in 2015 and sets clear goals and objectives for the FAA's cybersecurity program. These responsibilities are all accomplished through the collaboration of AFN, ATO, ANG, the Office of Aviation Safety (AVS), the Office of Airports, the Office of Security & Hazardous Materials Safety, and the Department of Transportation (DOT) CISO as members of the FAA CSC. With the input of these groups, other FAA offices as needed, and oversight of the CSC by senior FAA officials,

the FAA continues to review, update, and maintain the framework to support a more cyber-secure and resilient aviation ecosystem.

Following the establishment of the CSC, Congress continued to recognize the growing significance of cyber-threats. In 2016, Congress directed the FAA to develop a comprehensive strategic framework to reduce cybersecurity risks to the NAS, civil aviation, and agency information systems. Congress also directed the FAA to establish a cybersecurity research and development plan for the NAS, clarify cybersecurity roles and responsibilities of FAA offices and employees, identify and implement actions to reduce cybersecurity risks to air traffic control systems, and assess the cost and timeline of developing and maintaining an agency-wide cybersecurity threat model.[2] In response to the mandate, the FAA expanded its Cybersecurity Strategy and it is updated annually. The Cybersecurity Strategy discusses in detail the FAA's five goals which are: 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.

In 2018, Congress directed the FAA to assess the Cybersecurity Strategy for risks, review its objectives, and assess the FAA's level of engagement with stakeholders in carrying out the Strategy.[3] Although the FAA found the Cybersecurity Strategy's framework to be fundamentally sound, modifications were made to align it with other executive branch cyber

[2] Pub. Law No. 114-190, § 2111.
[3] Pub. Law No. 115-254, § 509.

initiatives, such as the National Cybersecurity Strategy and the National Strategy for Aviation Security. Enhancements were made to address the growing use of cloud and "as-a-service" technologies. The Cybersecurity Strategy was also modified to reflect efforts to improve response times in mitigation of internet-facing vulnerabilities, as well as cyber hygiene principles. It was strengthened by including a focus on external stakeholder engagement activities, including information-sharing and best practices around aviation cybersecurity.

Further, in response to a March 2019 DOT Office of Inspector General audit of FAA's Cybersecurity Strategy, the FAA finalized the application of its cyber risk model to support its air traffic mission and related systems, and established priorities for research and development activities on cybersecurity. These efforts have improved the FAA's ability to maintain up-to-date capabilities necessary for identifying and addressing rapidly evolving cyber threats.

FAA's Cybersecurity Role in the Aviation Ecosystem

When discussing cybersecurity as it relates to aviation, the FAA frequently refers to the "aviation ecosystem." Aspects of the aviation ecosystem include aircraft, air carriers, airports, air traffic operations, maintenance facilities and the personnel that carry out the functions for each. Although there is some overlap of cyber responsibilities with other participants for certain parts of the ecosystem, the FAA has safety oversight responsibilities for aircraft design, manufacturing and testing of aeronautical products, production, the continuous operational safety of certified products, and the certification of airmen and maintenance personnel. This includes components installed in aircraft, such as avionics. These responsibilities require the FAA to routinely engage with other aviation cybersecurity stakeholders including the private sector and other executive branch agencies that may have cyber responsibilities in the aviation ecosystem.

With respect to FAA's safety oversight responsibility in certificating aircraft, modern airplanes are designed and equipped with safety-enhancing systems that enable improved communications and navigation information. These systems rely on connectivity between an airplane and ground or space-based infrastructure. The reliance upon such connectivity creates cyber risks and, since such risks could affect the airworthiness of the aircraft, requires that such risks be addressed during the certification process. As part of the FAA's certification practices for standard category aircraft, cybersecurity risk assessments are conducted by the applicant when they apply for design certification or a change to a previously certified product. The FAA relies upon its broad safety regulatory authority to ensure that cyber risks are managed through the application of applicant-specific "special conditions" that require critical aircraft systems to be protected from adverse intentional unauthorized electronic interference. The FAA issues special conditions, which are rules of particular applicability, when the current airworthiness regulations do not contain adequate or appropriate safety standards for a novel or unusual design feature. The FAA addresses cybersecurity safety issues in much the same way as all safety issues, by monitoring safety impacts using a data-driven methodology. In response to an October 2020 Government Accountability Office report, the FAA conducted an initial cybersecurity risk assessment of avionic systems.[4] The FAA intends to do an in-depth analysis of our oversight responsibilities with respect to current and evolving avionics. At the request of the FAA, the Aviation Rulemaking Advisory Committee made 30 recommendations on Aircraft Systems Information Security and Protection. To date, the FAA has updated policy, standards and industry guidance for certifying critical aircraft systems.

[4] https://www.gao.gov/assets/gao-21-86.pdf.

The FAA also has a direct operational role in the air traffic aspect of the aviation ecosystem and manages cyber threats to the NAS Domain through ATO. The NAS Domain consists of over a hundred systems and an ever-growing networking infrastructure. The networking infrastructure is dedicated to NAS Domain operations and segregated from non-NAS infrastructures via secure monitored gateways. The NAS Domain provides five major FAA mission-critical services that directly support air traffic control: automation, communications, navigation, surveillance, and weather. ATO is responsible for air navigation services in all U.S.-controlled airspace and performs maintenance services for all NAS Domain systems. ATO is responsible for NAS Domain operational cybersecurity and provides the identification, protection, detection, response, and recovery capabilities to ensure continued NAS Domain operations under a range of cyber conditions. Further, in support of its cyber responsibilities for the NAS, in 2015, the FAA established the Cyber Test Facility, or CyTF, to assess cyber threats and vulnerabilities and conduct cyber testing and evaluation.

FAA's Coordination with Other Stakeholders in the Aviation Ecosystem

One of the major components of the FAA's Cybersecurity Strategy is focused on the FAA's continual effort to build and maintain relationships with, and provide guidance to, external partners in government and industry to sustain and improve cybersecurity in the aviation ecosystem. Building trust between the FAA and aviation cybersecurity stakeholders is critical to the success of building an aviation cybersecurity framework that enhances defense, reaction, and recovery from a cyber-incident and improves resilience. An example of the FAA's efforts in this area is the establishment of the Aviation Cyber Initiative (ACI) interagency task force. In May 2019 the Secretaries of Transportation, Homeland Security, and Defense chartered ACI as a forum for coordination and collaboration among federal agencies on a wide range of activities

aimed at cyber risk reduction within the aviation ecosystem. Such activities include research, development, testing, evaluation initiatives relating to aviation cybersecurity, engaging with stakeholders on activities for reducing cyber risks, and seeking potential improvement opportunities and risk mitigation strategies. The task force is tri-chaired by the three Departments, with the FAA representing the DOT on the task force. Some of the key areas for ACI working groups involve efforts to increase information sharing among ecosystem stakeholders—including airports and airlines, participation in inter-agency cyber exercises, and the development of risk mitigation strategies and guidance to improve and standardize risk management across the aviation ecosystem.

FAA's outreach, collaboration, and coordination with other stakeholders in the aviation ecosystem is not limited to its participation in ACI, and the FAA will continue to support information sharing efforts within the aviation industry to develop information security standards and best practices consistent with the National Institute of Standards and Technology Cybersecurity Framework. This engagement recognizes the increasingly interconnected nature of aviation information systems from the flight deck to air traffic control and air carrier operations, which necessitate innovative and collaborative solutions to secure them. Additionally, one-on-one engagements with industry groups and standards bodies are essential to ensure comprehensive cybersecurity policy and guidance for manufacturers and operators of aircraft. Further, the FAA will continue to actively engage with stakeholders around the globe to raise awareness of cybersecurity issues relevant to the aviation ecosystem and support initiatives to address cyber threats and vulnerabilities in a coordinated and collaborative manner.

FAA's Cybersecurity Workforce

One of the overarching goals of the FAA's Cybersecurity Strategy is to continue building and maintaining the agency's workforce capabilities for cybersecurity. Congress also recognized the importance of this effort and in 2018 directed the FAA to enter into an agreement with the National Academy of Sciences to conduct a study on the FAA cybersecurity workforce in order to develop recommendations to increase its size, quality, and diversity.[5] In June 2021, the FAA received the results of the Cyber Workforce Study, conducted by the National Academy of Sciences. The study identified key challenges facing the FAA's cyber workforce, it noted opportunities for strengthening that workforce, and made recommendations to help the FAA capitalize on those opportunities and address the challenges. For example, the study emphasized the importance of the FAA's ability to anticipate the need to continually retool the cybersecurity skills of its workforce given the rapidly changing nature of the challenge. It noted that the FAA cannot assume that today's cyber knowledge and skills will be sufficient to meet the needs of the future. The FAA recognizes that leveraging training and reskilling for the workforce will be a powerful tool for the FAA to grow and maintain the cyber skills needed now and in the future. The FAA also embraces the value of workforce training through participation in exercises. For example, the FAA regularly exercises its incident response plan to ensure familiarity with communications and escalation procedures. These internal exercises provide valuable experience for staff and increase the level of preparedness to respond to a cyber-incident. The FAA will continue to examine where expanding internal exercises will benefit preparedness.

[5] Pub. Law No. 115-254, § 549.

Finally, many of the recommendations in the National Academy of Science study are consistent with the FAA's cybersecurity strategic objectives, and many others align with broader ongoing FAA workforce development, diversity, and recruitment efforts. As technology and systems continue to evolve to meet the aviation challenges of tomorrow, so must our workforce. The FAA recognizes that a diverse pool of talent is critical to finding the right people for the right job at the right time. We also recognize that competitiveness in cybersecurity hiring and retention is important in order to attract and retain top talent. The FAA will use all of its federal recruiting, hiring and retention capabilities to continue building and to maintain the FAA cybersecurity workforce.

Conclusion

Chair DeFazio, Ranking Member Graves, and Members of the Committee, the FAA's cybersecurity responsibilities and our strategy to implement those responsibilities has expanded and evolved significantly over the years. Our efforts to address cybersecurity challenges have benefited from congressional oversight, our own initiatives, and our cooperative efforts with other executive branch agencies. As the technology of the aviation ecosystem evolves, we expect that cybersecurity will continue to be a growing challenge and a significant aspect of both aviation safety and the efficient use of airspace. We look forward to keeping Congress informed of our progress on all aspects of cybersecurity. I would be happy to answer any questions you may have.