Airlines for America®

We Connect the World

Testimony

AVIATION CYBERSECURITY THREATS
STATEMENT OF MARTY REYNOLDS, BRIGADIER GENERAL, USAF (RETIRED),
MANAGING DIRECTOR FOR CYBERSECURITY, AIRLINES FOR AMERICA
BEFORE THE
U.S. SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION COMMITTEE

September 18, 2024

Airlines for America (A4A) and our member airlines[1] appreciate the opportunity to testify and discuss the significant emphasis and investment our industry places on addressing cybersecurity challenges in an everchanging cyber threat environment. We thank the Committee for holding this important and timely hearing. There are no "silver bullets" for addressing cybersecurity, but rather, the best, mature cybersecurity programs are risk-based, threat-informed and constantly evolving to stay ahead of a dynamic threat landscape. Our member's cybersecurity programs and investments are based on these foundational principles.

Commitment

Airlines fully recognize that cyber security is one of the greatest challenges facing all critical infrastructure sectors. Airlines continue to make significant investments in information technology (IT) infrastructure and cybersecurity along with consistently partnering with the federal government and other private sector stakeholders to share information, best practices and lessons learned.

- **Investment:** Airlines take cybersecurity very seriously and are naturally incentivized to invest in their cyber infrastructure to ensure that operations are safe and secure. The safety, security and privacy of passengers and crew are the industry's highest priorities.
    - From 2018-2023, 13 U.S. passenger airlines spent ~$36.5 billion ($6.1 billion per year) on IT, including $7.4 billion in 2023, for IT labor/consulting/equipment/software, to bolster systems resiliency and to make it easier for travelers to shop for tickets and other services; check in for their journeys and navigate airports; check or track bags; modify itineraries; redeem vouchers/loyalty points; and stay apprised of flight status during irregular operations.
    - Airlines' cybersecurity investments include, but are not limited to: identification, prevention, detection, governance, threat and vulnerability management, incident response and recovery.
    - In addition to airlines' full time cyber security employees and other internal resources focused on cybersecurity, airlines use an array of third-party cyber security professionals and contractors, some of whom provide the same services across other industries and government.
    - A4A members invest their time and expertise as critical leaders in developing new and/or updating industry standards. These efforts include improving risk assessments, aircraft cybersecurity and digital information security. In addition, A4A members have created working groups focused on implementing Transportation Security Administration (TSA), Federal Aviation Administration (FAA) and Department of Defense (DoD) regulatory

[1] *See* A4A's members are: Alaska Air Group, Inc.; American Airlines Group, Inc.; Atlas Air Worldwide Holdings, Inc.; Delta Air Lines, Inc.; FedEx Corp.; Hawaiian Airlines; JetBlue Airways Corp.; Southwest Airlines Co.; United Airlines Holdings, Inc.; and United Parcel Service Co. Air Canada is an associate member.

requirements. These working groups also work closely with these regulators to ensure compliance implementation meets the regulatory intent while future requirements are informed by our operator's experiences and recommendations.

- **Information Sharing:** The industry supports and engages in a strong partnership of information sharing with the federal government and other stakeholders. Specifically, A4A members participate in and contribute to regular and frequent engagement with:
  - The Office of the National Cyber Director (ONCD), Federal Aviation Administration (FAA), Department of Homeland Security (DHS), Transportation Security Administration (TSA), Cybersecurity and Infrastructure Security Agency (CISA), Department of Defense (DoD), law enforcement, the intelligence community and other agencies;
  - The Defense Industrial Base, National Defense Transportation Association, Aviation Information Sharing and Analysis Center (A-ISAC), International Air Transport Association (IATA), International Civil Aviation Organization (ICAO), and other cyber-related communities; and
  - With the Original Equipment Manufacturers (OEMs) to further understand and prevent possible threats.

  A4A airlines are also active members of the A-ISAC mentioned above, involving the senior-most cybersecurity leader for each organization (most often the Chief Information Security Officer (CISO)) and threat intelligence analysts from each organization. The A-ISAC is focused on cybersecurity threat intelligence sharing to help assure the cybersecurity resiliency of the aviation industry. Airlines play a leadership role in A-ISAC and are deeply involved in working groups that address potential enterprise and aircraft vulnerabilities.

Recommendations

Harmonize Federal Requirements: A4A believes that protecting critical infrastructure requires consistent, streamlined and harmonized cybersecurity requirements. As a starting point, we strongly encourage Congress and the Administration to prioritize the harmonization of cybersecurity incident reporting requirements, especially before introducing any new requirements. The current practice of requiring multiple reports to different federal agencies is a significant and unnecessary burden on industry that reduces the effectiveness of voluntary and mandatory reporting frameworks and increases the likelihood of noncompliance.

- **Existing Cybersecurity Incident Reporting Disharmony:** In the Department of Homeland Security's (DHS) report, *Harmonization of Cyber Incident Reporting to the Federal Government*,[2] the authors identified 45 federal cybersecurity incident reporting requirements currently in effect. They also identified seven proposed rules, five potential new requirements under consideration and one future rule (*Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA)). Other than CIRCIA, none of these 58 cyber incident reporting requirements addresses harmonization or contemplates streamlining reporting requirements across federal agencies.

  Although the aviation industry is not subject to all 58 reporting requirements, airlines are currently subject to 10 different federal departments and agencies existing or proposed, mandatory and

[2] DHS Congressional Report, *Harmonization of Cyber Incident Reporting to the Federal Government,* September 19, 2023.

voluntary incident reporting frameworks. These federal agency and department frameworks include:

1. **Federal Aviation Administration (FAA)** – Mandatory Reporting (Advisory Circular 119-1A, "*Aircraft Network Security Program*," 28 September 2023);

2. **Transportation Security Administration (TSA)** – Mandatory Reporting (Standard Security Program Change, 10 January 2022);

3. **Department of Defense (DoD)** – Mandatory Reporting (Defense Federal Acquisition Regulations Supplement (DFARs) 252.204-7012 and 10 U.S.C. § 391 - U.S. Code - Unannotated Title 10. Armed Forces § 391);

4. **U.S. Transportation Command (USTRANSCOM)** – (General Cyber Security Requirements in USTRANSCOM Civil Reserve Aircraft Fleet (CRAF) contract, Appendix 6);

5. **Customs and Border Protection (CBP)** – Mandatory Reporting (Cargo Systems Messaging Service (CSMS) #5285040 – "*Reporting a Cybersecurity Event to CBP*," 12 September 2022 and CSMS #60261003);

6. **Security and Exchange Commission (SEC)** – Mandatory Reporting (*Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies* (In Effect on September 5, 2023)):

7. **Cybersecurity and Infrastructure Security Agency (CISA)** – Voluntary Reporting (*Cybersecurity Information Sharing Act* (CISA) of 2015), pending mandatory reporting (*Cyber Incident Reporting for Critical Infrastructure Act* (CIRCIA) of 2022);

8. **General Services Administration (GSA)** – Mandatory Reporting ((Federal Acquisition Regulations (FAR) subpart 4.4 & 52.204-232, C.F.R part 117) & (32 C.F.R 117.8)).

9. **Federal Bureau of Investigation (FBI)** – Voluntary Reporting (Report a Crime or Fraud); and

10. **National Aeronautics and Space Administration (NASA)** – Mandatory Reporting ((FAR subpart 4.4 & 52.204-232, C.F.R part 117) & (32 C.F.R 117.8)).

It is important to note that the requirements of these ten federal agencies differ on definitions, thresholds, processes, timelines, data protections, compliance regimes and content requirements. Although the federal government probably did not intend to create an environment where 45 cybersecurity incident reporting frameworks with divergent requirements are in effect, it is the environment regulated entities must currently navigate to ensure compliance. For sectors like transportation, with numerous regulators and relationships across sectors, this complex patchwork of disharmonized cybersecurity incident reporting requirements is especially burdensome. Requirements that take critical resources away from identifying, preventing, detecting, responding and recovering from cybersecurity incidents are not the best use of cybersecurity resources.

Finally, harmonization of incident reporting is a good first step, but harmonization of mandatory measures and compliance frameworks are also critically important. A4A supports ONCD's efforts to harmonize cybersecurity requirements across the federal government. Senator Peters and Senator

Lankford's recent proposal, S. 4630, the *Streamlining Federal Cybersecurity Regulations Act*, is also promising, as it would address the challenges associated with multiple regulatory regimes by establishing an interagency Harmonization Committee at the ONCD. Ensuring all mandatory requirements are streamlined and harmonized is in the best interest of regulators and operators, and it will lead to the best outcomes and drive down risk. If harmonization is not possible, then agencies should support a reciprocity framework that reduces unnecessary burdens and allow regulated parties to prioritize critical resources on a threat-based, risk-informed approach.

Improve Information Sharing: Information sharing among aviation regulators, the intelligence community, and private stakeholders is foundational to the safety, security and resiliency of the transportation system aviation subsector. Information sharing is necessary for both:

- Real-time intelligence and information used to protect aviation systems from existing and emerging threats; and

- To inform policy development, verify the effectiveness of policy outcomes, and determine if policy changes are necessary to stay ahead of evolving threats and risks.

However, the existing information sharing processes lack the speed necessary for relevance and do not consistently validate if existing policies and regulatory requirements achieve their desired policy outcomes.

Although federal agencies have made strides to improve information sharing such as multi-agency threat bulletins, information sharing among federal agencies and with the aviation sector needs to improve. The information airlines receive from federal agencies is often not timely or consistent. Additionally, it is not clear processes exist to rapidly update regulatory requirements at a speed necessary to stay ahead of evolving threats. We look forward to continuing to work with aviation regulators, the intelligence community and Congress to improve information sharing.

Conclusion

A4A supports cybersecurity policies and measures that promote a safe, secure and resilient U.S. airline industry and air transportation environment. As cybersecurity becomes increasingly important to aviation safety and security, it requires effective policies, practices and processes, as well as shared, mutual cybersecurity goals among air carriers, Congress and the rest of the federal government. Critical infrastructure sectors, like aviation, are best positioned when cybersecurity regulations and oversight are consistent and harmonized across the federal government. The best cybersecurity programs are those that are threat- and risk-based, data-informed, outcome-focused and flexible enough to address evolving threats. Federal cybersecurity policies and measures should likewise share these same principles.

We look forward to working with the Committee on shared cybersecurity challenges and thank you for the opportunity to discuss our role and involvement, along with recommendations to improve our cyber framework.