Airlines for America®

We Connect the World

Testimony

‘ENHANCING CYBERSECURITY BY ELIMINATING INCONSISTENT REGULATIONS’
STATEMENT FOR THE RECORD OF AIRLINES FOR AMERICA BEFORE THE HOUSE COMMITTEE ON OVERSIGHT AND ACCOUNTABILITY, SUBCOMMITTEE ON CYBERSECURITY, INFORMATION TECHNOLOGY, AND GOVERNMENT INNOVATION

July 25, 2024

On behalf our members[1], Airlines for America (A4A) submits this written testimony for the record for the House Oversight and Accountability Committee’s hearing on *Enhancing Cybersecurity by Eliminating Inconsistent Regulations*. We thank the Committee for holding this important hearing as harmonizing cybersecurity incident reporting requirements across the Federal Government is much needed and long overdue.

A4A supports policies and measures that promote safety, security and a healthy U.S. airline industry including those dealing with cybersecurity. Cybersecurity is 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. As an industry with multiple Federal regulators and contractors, we have concerns with the lack of harmonization of cybersecurity incident reporting across Federal agencies and believe improving harmonization of Federal policies will lead to better outcomes for both the private and public sectors.

A4A believes that protecting critical infrastructure requires consistent, streamlined and harmonized cybersecurity incident reporting requirements and 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 Dis-Harmony

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 subject to **10 different** Federal departments and agencies existing or proposed, mandatory and voluntary incident reporting frameworks. These Federal agency and department frameworks include:

[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.

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

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 contracts);

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 (C*ybersecurity 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);

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)); and

It is important to note, these 10 different Federal agency's and department's requirements 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 dis-harmonized cybersecurity incident reporting requirements is especially burdensome.

Harmonization Recommendations

While we are encouraged by recent Office of the National Cyber Director (ONCD) and CISA efforts to discuss harmonization across the Federal Government, we believe much more can and should be done. Specifically, we recommend the Federal Government take the following actions:

- Create and adopt a single reporting framework that includes agreed upon reporting definitions, threshold, process, timeline, data protections, compliance regime and content requirements.

- The Administration, independent regulators and Congress must prioritize cybersecurity incident reporting harmonization before any new cybersecurity requirements are implemented including proposed regulations or legislation for contractors who handle Federal information.

- Congress should remove any legal or statutory barriers to harmonization.

- The Administration and Congress should work with industry to pass legislation that balances regulatory compliance with consensus standards and incentives.

- Congress should pass legislation authorizing a Presidential designee to convene independent regulatory agencies to exchange best practices and coordinate cybersecurity incident reporting.

- Provide CISA with the necessary resources to implement CIRCIA and any future statutory incident reporting requirements.

Conclusion

Critical infrastructure sectors are best positioned when cybersecurity regulations and oversight are consistent 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. The current state of Federal cybersecurity incident reporting is inefficient, confusing, does not improve information sharing nor lead to better outcomes. The current state of cybersecurity incident reporting dis-harmonization was created by the Federal Government, but the Federal Government is also uniquely positioned to fix cybersecurity incident reporting harmonization, however, it will take a concerted effort by many to efficiently and effectively put in place a harmonized framework.

Thank you for the opportunity to raise concerns and provide recommendations to improve Federal harmonization of cybersecurity incident reporting. We stand ready to work with the Committee and other stakeholders to find practical solutions to harmonize cybersecurity incident reporting.