Airlines for America®

We Connect the World

April 10, 2023

Ms. Christina A. Walsh
TSA PRA Officer, Information Technology, TSA-11
Transportation Security Administration
6595 Springfield Center Drive
Springfield, VA 20598-6011

Dear Ms. Walsh,

Thank you for the opportunity to provide comments to the Transportation Security Administration's (TSA) information collection request (ICR) on cybersecurity measures for surface modes.[1] We appreciate that TSA has requested public comments on enhancing surface cyber risk management, because TSA's aviation sector cybersecurity regulatory requirements are informed by TSA's earlier work with the surface sector. Although we are not regulated by TSA's rail security directives (SD) (SD 1580-21-01 series, *Enhancing Rail Cybersecurity* and SD 1582-21-01 series *Enhancing Public Transportation and Passenger Railroad Cybersecurity)*, we are providing specific recommendations that we believe will improve cybersecurity for all transportation modes. We recommend TSA consider the following:

a. **Harmonize cybersecurity regulatory requirements with other federal regulatory agencies**. All transportation modes have touch points with multiple regulatory agencies. We recommend TSA coordinate its proposed cybersecurity regulatory actions with other regulators and agencies that are also mandating cybersecurity requirements on transportation operators. For the aviation sector, these include the Department of Defense, Securities and Exchange Commission, Federal Bureau of Investigations, U.S. Customs and Border Protection, and Cybersecurity and Infrastructure Security Agency, to name a few. TSA's regulatory approach, scope and applicability overlaps with these regulators and agency's existing and proposed cybersecurity requirements. Inconsistencies or conflicts must be avoided to prevent both security and compliance issues.

b. **Harmonization must consider other regulatory requirements beyond cybersecurity**. TSA's cybersecurity requirements will impact other regulatory requirements. For example, TSA was correct to consider aircraft outside of its scope of proposed aviation cybersecurity requirements, given the impact on the FAA's safety, airworthiness and aircraft certification requirements. A4A does not support TSA regulating aircraft and aircraft support information

[1] March 8, 2023 (FR Docket 2023-04859).

systems because it clearly conflicts with existing FAA requirements. Conflicts such as this highlight the need for TSA to discuss its cyber risk management program objectives, measures and goals with other regulators to ensure transportation operators are not required to select among conflicting regulations at the risk of noncompliance with a regulator's requirements.

c. **Modal equity should not drive sector policies**. Although many cybersecurity practices and frameworks are applicable across transportation modes, the ecosystems, controls, contracts and a host of other differences make absolute model equity impractical. For example, although the aviation sector uses operational technology, it is not as dependent upon OT systems for operational execution as other modes of transportation. Over emphasizing controls, such as IT/OT segmentation, is less important than emphasizing outcomes more appropriate to this specific sector.

d. **When modal equity does make sense, bring all modes together when developing shared definitions, frameworks and processes**. For example, definitions such as "critical cyber systems" are foundational to all modes of transportation, yet other transportation sectors did not have an opportunity to provide comments and recommendations during the surface sector's deliberations. Instead, the definition discussed with the surface sector was simply carried over to the aviation sector.

e. **Use accepted standard definitions**. We recommend all modes of transportation use the following definitions:

  i. **Critical cyber system**: "Any Information Technology (IT) or Operational Technology (OT) system whose compromise, as a result of a malicious cyber activity, would result in substantial operational disruption." TSA's current definition of "Critical Cyber Systems" is not founded on existing lexicon within statute or standards organizations such as NIST.

  ii. **System** (Glossary | CSRC (nist.gov)): "Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Note: Systems may also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems. Systems may include IT and OT systems."

  iii. **Compromise** (Glossary | CSRC (nist.gov)): "Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred."

  iv. **Malicious cyber activity** (Glossary | CSRC (nist.gov)): "Activities, other than those authorized by or in accordance with U.S. law, that seek to compromise or impair the confidentiality, integrity, or availability of computers, information or communications systems, networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon."

v. **Operational Disruption** (Glossary | CSRC (nist.gov)): "An unplanned event that interrupts operational events, activities, or processes for a length of time." This definition does not include a threshold for reporting or taking specific actions. TSA's proposed definition focuses on impacts to networks and systems and not on operational activities, events or processes. For example: "that results in...or indicates unauthorized access to, or malicious software present on, critical information technology systems." The unauthorized access or existence of malicious software does not equal an operational disruption. Another example, the loss of data, does not equate to operational disruptions.

vi. **Cybersecurity Incident** (Cyber Incident Reporting for Critical Infrastructure Act of 2022): "the term 'incident' means an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or actually or imminently jeopardizes, without lawful authority, an information system; does not include an occurrence that imminently, but not actually, jeopardizes— (i) information on information systems; or (ii) information systems."

vii. **Disruption** (disruption - Glossary | CSRC (nist.gov)): "An unplanned event that causes an information system to be inoperable for a length of time (*e.g.*, minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction)."

viii. **IT System**. This term is not in NIST, CIRCIA, or 44 U.S.C § 3502. The better term and definition is "Information System," which is "a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information; and includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers."

ix. **Operational Technology** (NIST SP 800-172): "Hardware and software that detects or causes a change through the direct monitoring or control of physical devices."

x. **Unauthorized Access** (NIST SP 800-172): Unauthorized Access of an Information Technology or Operational Technology System "means (1) the unauthorized logical or physical access, by a person, without permission to and Information Technology System or Operational Technology System; or (2) access that violates stated security policies."

xi. **Maintenance** (NIST SP 800-82 Rev. 2 from The Automation, Systems, and Instrumentation Dictionary): "Any act that either prevents the failure or malfunction of equipment or restores its operating capability."

f. **Ensure the cyber risk management program provides outcome-focused objectives associated with examples or recommended measures**. Controls are different from outcomes. Less emphasis should be placed on prescriptive measures. Instead, TSA must provide clear outcome-focused objectives including measurable outcomes. Measuring how well an organization implements prescriptive standards is not true performance-based management.

g. **Provide operators the flexibility to select the right measures based on their risk assessment and the evolving threat**. As a point of reference, according to a recent survey by SpyCloud, cyber actors are evolving their approach rapidly and getting ahead of static best practices. "*The tools and plans companies invest in to prevent ransomware do not appear to be working. Many have relied heavily on classic solutions like multifactor authentication and data backup systems, overlooking other issues like compromised web sessions and stolen login credentials sold on the dark web*." Allowing operators to dynamically select the best measures to achieve TSA's outcome-focused objectives is a significantly better approach than implementing a static, checklist-centered cybersecurity program. This flexibility allows operators to stay ahead of motivated and adaptive adversaries.

h. **Adopt a standardized cybersecurity framework (e.g., National Institute of Science and Technology's (NIST) Cybersecurity Framework (CSF)) to ensure outcome-focused objectives do not evolve into a checklist compliance framework**. Checklist compliance conflicts with NIST's CSF recommendations which states, "Security and privacy control assessments are not about checklists, simple pass/fail results, or generating paperwork to pass inspections or audits. Rather, control assessments are the principal vehicle used to verify that selected security and privacy controls are implemented and meeting stated goals and objectives." (NIST 800-53A). TSA can help by providing clear goals and objectives, and by granting operators the flexibility to select security and privacy measures and controls. Absent this adoption, operators will have to construct a compliance program that focuses on complying with a static checklist and less on dynamic, threat-informed cybersecurity measures.

i. **Provide the data, analysis, cybersecurity framework, and threat information TSA used to determine the performance-based outcomes**. Transportation operators know their systems, data, processes, and governance structures best, and they use threat-informed, risk-based approaches when developing and implementing their cybersecurity programs. Having the foundational information TSA used to select the outcomes and measures ensures operators can meet TSA's intent. Absent this information, operators are unable to align with TSA's priorities and threats to critical cyber systems.

j. **Avoid static implementation plans**. The process of annually updating prescriptive measures and static implementation plans is too slow for dynamic threats that are targeting critical infrastructure. In fact, shifting existing resources away from mature, threat informed, risk-based cybersecurity programs towards static, compliance-focused implementation plans may negatively impact cybersecurity.

k. **Develop a centralized compliance approach**. We urge the TSA to create a single, centralized group responsible for working with our information security experts at a corporate level, reviewing the TSA required documents and conducting any necessary compliance audits. We also recommend TSA consider a future third-party cybersecurity audit program, similar to the successful Third-Party Canine Program. It is critical that any auditors have the technical skills necessary to fully engage with transportation information security experts and be able to understand and approve equivalent measures and reasonable risk-informed alternatives.

l. **Ensure compliance and flexibility complement each other**. There are existing examples of assessment and certification processes that provide organizations with the flexibility to implement the right measures and controls based on their unique architecture, threats, risks, and industry processes. Examples include the payment card industry's (PCI) certification, TRANSCOM's assessment process, DoD's emerging Cybersecurity Maturity Model Certification and industry accepted standards (*e.g.*, NIST CSF). The applicability and scope of TSA's measures should not be based on a future compliance framework, but rather focused on how operators achieve TSA's performance-based outcomes.

m. **Retain a focus on collaboration and partnership with industry.** TSA's shift towards a cybersecurity regulatory and compliance posture is a significant divergence from decades of collaboration and partnership within the cybersecurity community. Cybersecurity is a team sport reliant on bi-directional information sharing, collaborative problem solving, development of industry standards and best practices, focusing on risks and threats, and a shared, common purpose. TSA's new scope and compliance-focused approach de-emphasizes these necessary attributes. For complex issues like cybersecurity, we recommend TSA brings together cross-sector experts to develop common lexicons and objectives before issuing requirements.

Developing complex policies for dynamic industries that face rapidly changing threats, emerging vulnerabilities, and an expanding domain requires more collaboration, not less. Cybersecurity requires collaboration beyond this single comment period. TSA has a rich history of collaborating with industry when there are emerging physical security threats. This is another opportunity to leverage this collaboration. The transportation industry and U.S. Federal government share the same goals—to ensure a safe, secure and resilient industry.

Sincerely,

Lauren Beyer

Lauren Beyer
Vice President, Security and Facilitation
Airlines for America