Transportation Security Administration

U.S. Department of Homeland Security
Transportation Security Administration
6595 Springfield Center Drive
Springfield, Virginia 20598

TSA-APPROVED SECURITY PROGRAM ADDENDUM

NUMBER	TSA-NA-21-05 – Non-SSI Measures
SUBJECT	Cybersecurity Incident Reporting
PROGRAM	49 CFR 1542.103
REFERENCE	Airport Security Program National Amendment
EFFECTIVE	January 10, 2022
EXPIRES	N/A

PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) issued TSA-NA-21-05: Cybersecurity Incident Reporting. In light of the cybersecurity threat to transportation and in conjunction with the Department of Homeland Security's (DHS) Cybersecurity Sprint for the Transportation sector, TSA developed these requirements in coordination with DHS, the Cybersecurity and Infrastructure Security Agency (CISA), and the Federal Aviation Administration (FAA).

TSA issued this change to clarify and improve requirements for airport operators to report cybersecurity incidents to the Federal Government. TSA incorporated the following requirements into TSA-NA-21-05. TSA has determined that the measures in this document are not Sensitive Security Information (SSI) under part 1520 of title 49, Code of Federal Regulations. The airport operator must incorporate this document as a non-SSI addendum to their ASP, which may be shared with interested entities.

This document identifies two critical actions. First, it requires airport operators to report cybersecurity incidents to CISA. Second, it requires the airport operator to designate a Cybersecurity Coordinator, who must be available to TSA and CISA 24/7 to coordinate cybersecurity practices and address any incidents that arise.

To avoid duplicate reporting, information provided to CISA pursuant to this document would be shared with TSA and may also be shared with the National Response Center and other agencies, including the Department of Transportation (DOT) and the Federal Aviation Administration (FAA), as appropriate. Similarly, information provided to TSA pursuant to this document would

be shared with CISA and may also be shared with the National Response Center and other agencies, including DOT and FAA, as appropriate.[1]

All information that must be reported to TSA or CISA pursuant to this document will be considered SSI subject to the protections of part 1520 of title 49, Code of Federal Regulations.

TSA may use the information, with company-specific data redacted, for TSA's intelligence-derived reports. TSA and CISA also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.

Airport operators must comply with these requirements in addition to and notwithstanding any other federal cybersecurity reporting requirements and processes. An airport operator that reports an incident covered by this document via another Federal cybersecurity reporting process is not relieved of its responsibility to comply with the reporting requirements established herein. The airport operator is not relieved of its responsibility to report safety-related matters, including those that may have a cybersecurity nexus, to the FAA directly where FAA regulations so require.

TERMS AND DEFINITIONS

Cybersecurity Incident: An event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the airport operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, benign).

Information Technology (IT) System: Any services, equipment, or interconnected system(s) or subsystem(s) of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of the airport operator to operate and maintain.

Operational Disruption: A deviation from or interruption of normal activities or operations that results in a loss of data, system availability, system reliability, or control of systems, or indicates unauthorized access to, or malicious software present on, critical information technology systems.

[1] Presidential Policy Directive (PPD) 41 calls for Federal cyber incident response agencies to share incident information with each other to achieve unity of governmental effort. *See* PPD-41 § III.D. Additionally, 6 U.S.C § 233(a) requires the Secretary of Homeland Security and other officials in the Department of Homeland Security to consult with the Administrator of the Federal Aviation Administration before taking any action that might affect aviation safety, air carrier operations, aircraft airworthiness, or the use of airspace. TSA is further required to work in conjunction with the Administrator of the Federal Aviation Administration with respect to any actions or activities that may affect aviation safety or air carrier operations. 49 U.S.C. § 114 (f)(13).

Operational Technology System: A general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the aviation sector and aviation critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, or pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.

Unauthorized Access of an Information Technology (IT) System or Operational Technology System: Access from an unknown source; unauthorized access by a third party or former employee; an employee accessing systems for which they are not authorized; and may include a non-malicious airport operator policy violation such as the use of shared credential by an employee otherwise authorized to access it.

APPROVED PROCEDURES

A. The airport operator must designate and use a primary and at least one alternate cybersecurity coordinator. The cybersecurity coordinator or alternate cybersecurity coordinator may also be the airport security coordinator (ASC), provided they meet the requirements set forth in Section A.2.:

   1) The airport operator must provide in writing to TSA via their FSD or designee, the names, titles, phone number(s), and email address(es) of the cybersecurity coordinator and alternate cybersecurity coordinator(s) by the effective date of this amendment or within seven days of any change in the information required by Section A.

   2) The cybersecurity coordinator and alternate cybersecurity coordinator(s) must:

      a. Be a U.S. citizen who is therefore eligible to seek a security clearance at the Secret Level;

      b. Serve as the primary contact for cyber-related intelligence information and cybersecurity-related activities and communications with TSA and the Cybersecurity and Infrastructure Security Agency (CISA);

      c. Be accessible to TSA and CISA 24-hours a day, seven-days a week;

      d. Coordinate cyber and related security practices and procedures internally; and

      e. Work with appropriate law enforcement and emergency response agencies.

B. The airport operator must report to the CISA cybersecurity incidents involving systems that the airport operator has the responsibility to operate and maintain, including:

   1. Unauthorized access to an Information Technology (IT) or Operational Technology (OT) system;

2. Discovery of malicious software on an IT or OT system;

3. Activity resulting in a denial of service to any IT or OT system;

4. A physical attack against the airport operator's network infrastructure (e.g., intentional fiber cuts etc.);

5. Any other cybersecurity incident that results in operational disruption to the airport operator's IT or OT systems or other aspects of the airport operator's systems or facilities, or otherwise has the potential to cause an operational disruption that adversely affects the safety and efficient transportation of persons and property traveling on flights from, to, or through the airport;

6. The airport operator's interface with applicable Department of Homeland Security IT systems, including but not limited to Secure Flight (SF).

C. The airport operator must report the information required in Section D. as soon as practicable, but no later than 24-hours after a cybersecurity incident is identified. Reports must be made to CISA Central using CISA's Reporting System form at: https://us-cert.cisa.gov/forms/report or by calling (888) 282-0870.[2] If the required information is not available at the time of reporting, the airport operator must submit an initial report within the specified timeframe and supplement as additional information becomes available. All reported information will be protected in a manner appropriate for the sensitivity and criticality of the information and is sensitive security information subject to the protections of part 1520 of title 49, Code of Federal Regulations.

D. In the report to CISA required by Section C., the airport operator must include the following information:

1. The name, telephone number, and email address of the reporting individual. The report must explicitly specify that the information is being reported in order to satisfy the reporting requirements in this amendment;

2. The affected airport operator, including identifying information and location;

3. A description of the threat, incident, or suspicious activity, to include:

   a. Earliest known date of compromise;

   b. Date of detection;

   c. Information about who has been notified and what action has been taken;

[2] CISA's Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handing of the security incidents the airport operator must report pursuant to this Amendment as well as the ability to conduct improved analysis.

d. Any relevant technical information observed or collected by the airport operator, such as malicious IP addresses, malicious domains, malware hashes and/or samples, or the abuse of legitimate software or accounts;

e. Any known threat information, to include information about the source of the threat or attack, if available.

4. A description of the incident's impact or potential impact on Information or Operational Technology systems and operations. This information must also include an assessment of actual, imminent, or potential impact to airport or flight operations, operational delays, and/or data theft that have or are likely to be incurred, as well as any other information that would be informative in understanding the impact or potential impact of the cybersecurity incident;

5. A description of all responses that are planned or under consideration, to include, for example, a reversion to manual backups, if applicable;

6. Actions and/or mitigation efforts taken in response (consistent with all applicable FAA and TSA regulations);

7. Any additional relevant information.

SCOPE AND DURATION OF APPROVAL

A. In accordance with 49 Code of Federal Regulations (CFR) 1542.105(c), this document amends the TSA-approved security program adopted by the airport operator in accordance with the requirements of 49 CFR 1542.103.

B. Changes to TSA-NA-21-05 may require a corresponding revision of this addendum. It is the responsibility of the airport operator to review this addendum when TSA issues an airport security program national amendment that revises relevant requirements. Consult your Federal Security Director or designee, as appropriate, to determine if revision of this addendum is required.

THOMAS L BUSH

Digitally signed by THOMAS L BUSH
Date: 2021.11.21 20:13:10 -05'00'

Thomas L. Bush
Acting Executive Assistant Administrator
Operations Support