TSA is issuing this change to clarify and improve requirements for airport operators to report cybersecurity incidents to the Federal Government. This Amendment would require two critical actions. First, it requires airport operators to report cybersecurity incidents to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

Second, it requires the airport operator to designate a Cybersecurity Coordinator who is required to 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 Amendment 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 Amendment would be shared with CISA and may also be shared with the National Response Center and other agencies, including DOT and FAA, as appropriate.

All information that must be reported to TSA or CISA pursuant to this Amendment is Sensitive Security Information (SSI) subject to the protections of part 1520 of title 49, Code of Federal Regulations. TSA may use the information, with airport operator-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 National Amendment via another Federal cybersecurity reporting process is not relieved of its responsibility to comply with the reporting requirements established in this National Amendment. In addition, nothing in this National Amendment relieves an airport operator 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. If an airport operator's ASP already addresses one or more of these requirements, the airport operator need only amend its ASP to the extent necessary to address those requirements not already in the ASP.

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.

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

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://uscert.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;
    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.