SUBCHAPTER D—MARITIME AND SURFACE TRANSPORTATION SECURITY

PART 1570—GENERAL RULES

Subpart A—General

Subpart B—Security Programs

Subpart C—Operations

Subpart D—Security Threat Assessments

AUTHORITY: 18 U.S.C. 842, 845; 46 U.S.C. 70105; 49 U.S.C. 114, 5103a, 40113, and 46105; Pub. L. 108–90 (117 Stat. 1156, Oct. 1, 2003), sec. 520 (6 U.S.C. 469), as amended by Pub. L. 110–329 (122 Stat. 3689, Sept. 30, 2008) sec. 543 (6 U.S.C. 469); Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1402 (6 U.S.C. 1131), 1405 (6 U.S.C. 1134), 1408 (6 U.S.C. 1137), 1413 (6 U.S.C. 1142), 1414 (6 U.S.C. 1143), 1501 (6 U.S.C. 1151), 1512 (6 U.S.C. 1162), 1517 (6 U.S.C. 1167), 1522 (6 U.S.C. 1170), 1531 (6 U.S.C. 1181), and 1534 (6 U.S.C. 1184).

SOURCE: 85 FR 16499, Mar. 23, 2020, unless otherwise noted.

Subpart A—General

§ 1570.1 Scope.

This part applies to any person involved in maritime or surface transportation as specified in this subchapter.

§ 1570.3 Terms used in this subchapter.

In addition to the definitions in §§ 1500.3, 1500.5, and 1503.202 of subchapter A, the following terms are used in this subchapter:

Adjudicate means to make an administrative determination of whether an applicant meets the standards in this subchapter, based on the merits of the issues raised.

Alien registration number means the number issued by the DHS to an individual when he or she becomes a lawful permanent resident of the United States or attains other lawful, non-citizen status.

Applicant means a person who has applied for one of the security threat assessments identified in this subchapter.

Commercial driver's license (CDL) is used as defined in 49 CFR 383.5.

Contractor means a person or organization that provides a service for an owner/operator regulated under this subchapter consistent with a specific understanding or arrangement. The understanding can be a written contract or an informal arrangement that reflects an ongoing relationship between the parties.

Convicted means any plea of guilty or nolo contendere, or any finding of guilt, except when the finding of guilt is subsequently overturned on appeal, pardoned, or expunged. For purposes of this subchapter, a conviction is expunged when the conviction is removed from the individual's criminal history record and there are no legal disabilities or restrictions associated with the expunged conviction, other than the fact that the conviction may be used for sentencing purposes for subsequent convictions. In addition, where an individual is allowed to withdraw an original plea of guilty or nolo contendere

and enter a plea of not guilty and the case is subsequently dismissed, the individual is no longer considered to have a conviction for purposes of this subchapter.

Determination of No Security Threat means an administrative determination by TSA that an individual does not pose a security threat warranting denial of an HME or a TWIC.

Employee means an individual who is engaged or compensated by an owner/operator regulated under this subchapter, or by a contractor to an owner/operator regulated under this subchapter. The term includes direct employees, contractor employees, authorized representatives, immediate supervisors, and individuals who are self-employed.

Federal Maritime Security Coordinator (FMSC) has the same meaning as defined in 46 U.S.C. 70103(a)(2)(G); is the Captain of the Port (COTP) exercising authority for the COTP zones described in 33 CFR part 3, and is the Port Facility Security Officer as described in the International Ship and Port Facility Security (ISPS) Code, part A.

Final Determination of Threat Assessment means a final administrative determination by TSA, including the resolution of related appeals, that an individual poses a security threat warranting denial of an HME or a TWIC.

Hazardous materials endorsement (HME) means the authorization for an individual to transport hazardous materials in commerce, an indication of which must be on the individual's commercial driver's license, as provided in the Federal Motor Carrier Safety Administration regulations in 49 CFR part 383.

Immediate supervisor means a manager, supervisor, or agent of the owner/operator to the extent the individual:

(1) Performs the work of a security-sensitive employee; or

(2) Supervises and otherwise directs the performance of a security-sensitive employee.

Imprisoned or *imprisonment* means confined to a prison, jail, or institution for the criminally insane, on a full-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity. Time spent confined or restricted to a half-way house, treatment facility, or similar institution, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity, does not constitute imprisonment for purposes of this rule.

Incarceration means confined or otherwise restricted to a jail-type institution, half-way house, treatment facility, or another institution on a full or part-time basis, pursuant to a sentence imposed as the result of a criminal conviction or finding of not guilty by reason of insanity.

Initial Determination of Threat Assessment means an initial administrative determination by TSA that an applicant poses a security threat warranting denial of an HME or a TWIC.

Initial Determination of Threat Assessment and Immediate Revocation means an initial administrative determination that an individual poses a security threat that warrants immediate revocation of an HME or invalidation of a TWIC. In the case of an HME, the State must immediately revoke the HME if TSA issues an Initial Determination of Threat Assessment and Immediate Revocation. In the case of a TWIC, TSA invalidates the TWIC when TSA issues an Initial Determination of Threat Assessment and Immediate Revocation.

Invalidate means the action TSA takes to make a credential inoperative when it is reported as lost, stolen, damaged, no longer needed, or when TSA determines an applicant does not meet the security threat assessment standards of 49 CFR part 1572.

Maritime facility has the same meaning as ''facility'' together with ''OCS facility'' (Outer Continental Shelf facility), as defined in 33 CFR 101.105.

Mental health facility means a mental institution, mental hospital, sanitarium, psychiatric facility, and any other facility that provides diagnoses by licensed professionals of mental retardation or mental illness, including a psychiatric ward in a general hospital.

Revocation means the termination, deactivation, rescission, invalidation, cancellation, or withdrawal of the privileges and duties conferred by an HME or TWIC, when TSA determines

an applicant does not meet the security threat assessment standards of 49 CFR part 1572.

Secure area means the area on board a vessel or at a facility or outer continental shelf facility, over which the owner/operator has implemented security measures for access control, as defined by a Coast Guard approved security plan. It does not include passenger access areas or public access areas, as these terms are defined in 33 CFR 104.106 and 105.106 respectively. Vessels operating under the waivers provided for at 46 U.S.C. 8103(b)(3)(A) or (B) have no secure areas. Facilities subject to 33 CFR chapter I, subchapter H, part 105 may, with approval of the Coast Guard, designate only those portions of their facility that are directly connected to maritime transportation or are at risk of being involved in a transportation security incident as their secure areas.

Security-sensitive employee, for purposes of this part, means ''security sensitive employee'' as defined in §1580.3, §1582.3, or §1584.3 of this title.

Security-sensitive job function, for purposes of this part, means a job function identified in appendix B to part 1580, appendix B to part 1582, and appendix B to part 1584 of this title.

Transportation Worker Identification Credential (TWIC) means a Federal biometric credential, issued to an individual, when TSA determines that the individual does not pose a security threat.

Withdrawal of Initial Determination of Threat Assessment is the document that TSA issues after issuing an Initial Determination of Security Threat, when TSA determines that an individual does not pose a security threat that warrants denial of an HME or TWIC.

[85 FR 16499, Mar. 23, 2020, as amended at 89 FR 35631, May 1, 2024]

§ 1570.5 Fraud and intentional falsification of records.

No person may make, cause to be made, attempt, or cause to attempt any of the following:

(a) Any fraudulent or intentionally false statement in any record or report that is kept, made, or used to show compliance with the subchapter, or exercise any privileges under this subchapter.

(b) Any reproduction or alteration, for fraudulent purpose, of any record, report, security program, access medium, or identification medium issued under this subchapter or pursuant to standards in this subchapter.

§ 1570.7 Security responsibilities of employees and other persons.

(a) No person may—

(1) Tamper or interfere with, compromise, modify, attempt to circumvent, or cause another person to tamper or interfere with, compromise, modify, or attempt to circumvent any security measure implemented under this subchapter.

(2) Enter, or be present within, a secured or restricted area without complying with the security measures applied as required under this subchapter to control access to, or presence or movement in, such areas.

(3) Use, allow to be used, or cause to be used, any approved access medium or identification medium that authorizes the access, presence, or movement of persons or vehicles in secured or restricted areas in any other manner than that for which it was issued by the appropriate authority to meet the requirements of this subchapter.

(b) The provisions of paragraph (a) of this section do not apply to conducting inspections or tests to determine compliance with this subchapter authorized by—

(1) TSA and DHS officials working with TSA; or

(2) The owner/operator when acting in accordance with the procedures described in a security plan and/or program approved by TSA.

§ 1570.9 [Reserved]

Subpart B—Security Programs

§ 1570.101 Scope.

The requirements of this subpart address general security program requirements applicable to each owner/operator required to have a security program under subpart B to 49 CFR parts 1580, 1582, and 1584.

§ 1570.103 Content.

(a) *Security program.* Except as otherwise approved by TSA, each owner/operator required to have a security program must address each of the security program requirements identified in subpart B to 49 CFR parts 1580, 1582, and 1584.

(b) *Use of appendices.* The owner/operator may comply with the requirements referenced in paragraph (a) of this section by including in its security program, as an appendix, any document that contains the information required by the applicable subpart B, including procedures, protocols or memorandums of understanding related to external agency response to security incidents or events. The appendix must be referenced in the corresponding section(s) of the security program.

§ 1570.105 Responsibility for Determinations.

(a) *Higher-risk operations.* While TSA has determined the criteria for applicability of the requirements in subpart B to 49 CFR parts 1580, 1582, and 1584 based on risk-assessments for freight railroad, public transportation system, passenger railroad, or over-the-road (OTRB) owner/operators are required to determine if the applicability criteria identified in subpart B to parts 1580, 1582, and 1584 apply to their operations. Owner/operators are required to notify TSA of applicability within 30 days of June 22, 2020.

(b) *New or modified operations.* If an owner/operator commences new operations or modifies existing operations after June 22, 2020, that person is responsible for determining whether the new or modified operations would meet the applicability criteria in subpart B to 49 CFR part 1580, 1582, or 1584 and must notify TSA no later than 90 calendar days before commencing operations or implementing modifications.

§ 1570.107 Recognition of prior or established security measures or programs.

Previously provided security training may be credited towards satisfying the requirements of this subchapter provided the owner/operator—

(a) Obtains a complete record of such training and validates the training meets requirements of § 1580.115, § 1582.115, or § 1584.115 of this subchapter as it relates to the function of the individual security-sensitive employee and the training was provided within the schedule required for recurrent training.

(b) Retains a record of such training in compliance with the requirements of § 1570.121 of this part.

§ 1570.109 Submission and approval.

(a) *Submission of security program.* Each owner/operator required under parts 1580, 1582, or 1584 of this subchapter to adopt and carry out a security program must submit it to TSA for approval in a form and manner prescribed by TSA.

(b) *Security training deadlines.* Except as otherwise directed by TSA, each owner/operator required under subpart B to part 1580, 1582, or 1584 of this subchapter to develop a security training program must—

(1) Submit its program to TSA for approval no later than June 21, 2021.

(2) If commencing or modifying operations so as to be subject to the requirements of subpart B to 49 CFR parts 1580, 1582, or 1584 after June 21, 2021, submit a training program to TSA no later than 90 calendar days before commencing new or modified operations.

(c) *TSA approval.* (1) No later than 60 calendar days after receiving the proposed security program required by subpart B to 49 CFR parts 1580, 1582, and 1584, TSA will either approve the program or provide the owner/operator with written notice to modify the program to comply with the applicable requirements of this subchapter. TSA will notify the owner/operator if it needs an extension of time to approve the program or provide the owner/operator with written notice to modify the program to comply with the applicable requirements of this subchapter.

(2) *Notice to modify.* If TSA provides the owner/operator with written notice to modify the security program to comply with the applicable requirements of this subchapter, the owner/operator must provide a modified security program to TSA for approval within the timeframe specified by TSA.

(3) TSA may request additional information, and the owner/operator must provide the information within the time period TSA prescribes. The 60-day period for TSA approval or modification will begin when the owner/operator provides the additional information.

(g) *Petition for reconsideration.* Within 30 days of receiving the notice to modify, the owner/operator may file a petition for reconsideration under §1570.119 of this part.

[85 FR 16499, Mar. 23, 2020, as amended at 85 FR 67683, Oct. 26, 2020; 86 FR 23632, May 4, 2021]

§1570.111 Implementation schedules.

(a) *Initial security training.* Each owner/operator required under parts 1580, 1582, or 1584 of this subchapter to adopt and carry out a security program must provide initial security training to security-sensitive employees, using the curriculum approved by TSA and in compliance with the following schedule.

(1) For security training programs submitted to TSA for approval on or before March 22, 2021, if the employee is employed to perform a security-sensitive function on the date TSA approves the program, then initial training must be provided no later than fifteen months after the date that TSA approves the owner/operator's security training program.

(2) For security training programs submitted to TSA for approval after March 22, 2021, if the employee is employed to perform a security-sensitive function on the date TSA approves the program, then initial training must be provided no later than twelve months after the date that TSA approves the owner/operator's security training program.

(3) If performance of a security-sensitive job function is initiated after TSA approves the owner/operator's security training program, then initial training must be provided no later than 60 calendar days after the employee first performs the security-sensitive job function.

(4) If the security-sensitive job function is performed intermittently, then no later than the 60th calendar day of employment performing a security-sensitive function, aggregated over a consecutive 12-month period.

(b) *Recurrent security training.* (1) Except as provided in paragraph (b)(2) of this section, a security-sensitive employee required to receive training under part 1580, 1582, or 1584 of this subchapter must receive the required training at least once every three years.

(2) If an owner/operator modifies a security program or security plan for which training is required under §1580.203(b), §1582.115(b), or §1584.115(b) of this subchapter, the owner/operator must ensure each security-sensitive employee with position- or function-specific responsibilities related to the revised plan or program changes receives training on the revisions within 90 days of implementation of the revised plan or program changes. All other employees must receive training that reflects the changes to the operating security requirements as part of their regularly scheduled recurrent training.

(3) The three-year recurrent training cycle is based on the anniversary calendar month of the employee's initial security training. If the owner/operator provides the recurrent security training in the month of, the month before, or the month after it is due, the employee is considered to have taken the training in the month it is due.

(c) *Extensions of time.* TSA may grant an extension of time for implementing a security program identified in subpart B to parts 1580, 1582, and 1584 of this subchapter upon a showing of good cause. The owner/operator must request the extension of time in writing and TSA must receive the request within a reasonable time before the due date to be extended; an owner/operator may request an extension after the expiration of a due date by sending a written request describing why the failure to meet the due date was excusable. TSA will respond to the request in writing.

[85 FR 16499, Mar. 23, 2020, as amended at 86 FR 23632, May 4, 2021]

§ 1570.113 Amendments requested by owner/operator.

(a) *Changes to ownership or control of operations.* Each owner/operator required under part 1580, 1582, or 1584 of this subchapter to adopt and carry out a security program must submit a request to amend its security program if, after approval, there are any changes to the ownership or control of the operation.

(b) *Changes to conditions affecting security.* Each owner/operator required under part 1580, 1582, or 1584 of this subchapter to adopt and carry out a security program must submit a request to amend its security program if, after approval, the owner/operator makes, or intends to make, permanent changes to any of the following procedures, measures, or other aspects of security or emergency response planning implemented by the owner/operator to address:

(1) Specific procedures implemented or used to prevent and detect unauthorized access to restricted areas designated by the owner/operator;

(2) Measures to be implemented in response to a period of heightened security risk, communicated through a DHS enhanced security notification, including the process used to notify all employees of changes in alert level status or requirements to implement specific elements of the security plan and verify that appropriate enhanced security measures have been implemented at all relevant locations.

(3) Emergency response plans, including:

(i) Coordinated response plans establishing procedures for appropriate interaction with State, local, and tribal law enforcement agencies, emergency responders, and Federal officials in order to coordinate security measures and plans for response in the event of a terrorist threat, attack, or other transportation security-related incident;

(ii) Specific procedures to be implemented or used by the owner/operator in response to a terrorist attack, including evacuation and communication plans that include individuals with disabilities; and

(iii) Additional measures to be adopted to address weaknesses in emergency response procedures identified during regular drills or exercises that test corporate capabilities to direct, coordinate, and execute prevention and response activities for terrorist attacks or other security threats, including tunnel evacuation procedures, if applicable.

(iv) Redundant and backup systems to ensure the continuity of operations of critical assets and infrastructure system in the event of a terrorist attack or other transportation security-related incident.

(c) *Changes to security training curriculum.* Each owner/operator required under part 1580, 1582, or 1584 of this subchapter to adopt and carry out a security program must submit a request to amend its security program if, after approval, the owner/operator makes, or intends to make, permanent changes to its security training curriculum required under part 1580, 1582, or 1584, including changes to address:

(1) Determinations that the security training program is ineffective based on the approved method for evaluating effectiveness in the security training program approved by TSA under subpart B of parts 1580, 1582, and 1584; or

(2) Development of recurrent training material for purposes of meeting the requirements in § 1570.111(b) of this part or other alternative training materials not previously approved by TSA.

(d) *Permanent change.* For purposes of this section, a ''permanent change'' is one intended to be in effect for 60 or more calendar days.

(e) *Schedule for requesting amendment.* The owner/operator must file the request for an amendment with TSA no later than 65 calendar days after the change in subsection (b) takes effect, unless TSA allows a shorter time period.

(f) *TSA approval.* (1) Within 30 calendar days after receiving a proposed amendment, TSA will, in writing, either approve or deny the request to amend. TSA will notify the owner/operator if it needs an extension of time to consider the proposed amendment.

(2) TSA may approve—

(i) An amendment to a security program if TSA determines that it is in the interest of the public and transportation security and the proposed

amendment provides the level of security required under this subchapter.

(ii) Modification to security training curriculum, including alternative training for purposes of meeting the recurrent training requirement, if all the required training elements are addressed and the material is consistent with the most recent iteration of the security program submitted to, and approved by, TSA (including amendments made to reflect relevant changes to operations and/or security measures and response plans).

(iii) TSA may request additional information from the owner/operator before rendering a decision.

(g) *Petition for reconsideration.* No later than 30 calendar days after receiving a denial, the owner/operator may file a petition for reconsideration under §1570.119 of this part.

§1570.115 Amendments required by TSA.

(a) *Notification of requirement to amend.* TSA may require amendments to a security program in the interest of the public and transportation security, including any new information about emerging threats, or methods for addressing emerging threats, as follows:

(1) TSA will notify the owner/operator of the proposed amendment, fixing a period of not less than 30 calendar days within which the owner/operator may submit written information, views, and arguments on the amendment.

(2) After TSA considers all relevant material received, TSA will notify the owner/operator of any amendment adopted or rescind the notice.

(b) *Effective date of amendment.* If TSA adopts the amendment, it becomes effective not less than 30 calendar days after the owner/operator receives the notice of amendment, unless the owner/operator disagrees with the proposed amendment and files a petition for reconsideration under §1570.119 of this part no later than 15 calendar days before the effective date of the amendment. A timely petition for reconsideration stays the effective date of the amendment.

(c) *Emergency amendments.* If TSA determines that there is an emergency requiring immediate action in the interest of the public or transportation security, TSA may issue an amendment, without the prior notice and comment procedures in paragraph (a) of this section, effective without stay on the date the covered owner/operator receives notice of it. In such a case, TSA will incorporate in the notice a brief statement of the reasons and findings for the amendment to be adopted. The owner/operator may file a petition for reconsideration under §1570.119 of this part; however, this does not stay the effective date of the emergency amendment.

§1570.117 Alternative measures.

(a) If in TSA's judgment, the overall security of transportation provided by an owner/operator subject to the requirements of 49 CFR part 1580, 1582, or 1584 are not diminished, TSA may approve alternative measures.

(b) Each owner/operator requesting alternative measures must file the request for approval in a form and manner prescribed by TSA. The filing of such a request does not affect the owner/operator's responsibility for compliance while the request is being considered.

(c) TSA may request additional information, and the owner/operator must provide the information within the time period TSA prescribes. Within 30 calendar days after receiving a request for alternative measures and all requested information, TSA will, in writing, either approve or deny the request.

(d) If TSA finds that the use of the alternative measures is in the interest of the public and transportation security, it may grant the request subject to any conditions TSA deems necessary. In considering the request for alternative measures, TSA will review all relevant factors including—

(1) The risks associated with the type of operation, for example, whether the owner/operator transports hazardous materials or passengers within a high threat urban area, whether the owner/operator transports passengers and the volume of passengers transported, or whether the owner/operator hosts a passenger operation.

(2) Any relevant threat information.

(3) Other circumstances concerning potential risk to the public and transportation security.

(e) No later than 30 calendar days after receiving a denial, the owner/operator may petition for reconsideration under § 1570.119 of this part.

§ 1570.119 Petitions for reconsideration.

(a) If an owner/operator seeks to petition for reconsideration of a determination, required modification, denial of a request for amendment by the owner/operator, denial to rescind a TSA-required amendment, or denial of an alternative measure, the owner/operator must submit a written petition for reconsideration that includes a statement and any supporting documentation explaining why the owner/operator believes TSA's decision is incorrect.

(b) Upon review of the petition for reconsideration, the Administrator or designee will dispose of the petition by affirming, modifying, or rescinding its previous decision. This is considered a final agency action.

§ 1570.121 Recordkeeping and availability.

(a) *Retention.* Each owner/operator required to have a security program under subpart B to parts 1580, 1582, and 1584 of this subchapter must—

(1) Retain security training records for each individual required to receive security training under §§ 1580.115, 1582.115, and 1584.115 that, at a minimum—

(i) Includes employee's full name, job title or function, date of hire, and date of initial and recurrent security training; and

(ii) Identifies the date, course name, course length, and list of topics addressed for the security training most recently provided in each of the areas required under §§ 1580.115, 1582.115, and 1584.115 of this subchapter.

(2) Retain records of initial and recurrent security training for no less than five (5) years from the date of training.

(3) Provide records to current and former employees upon request and at no charge as necessary to provide proof of training.

(b) *Electronic records.* Each owner/operator required to retain records under this section may keep them in electronic form. An owner/operator may maintain and transfer records through electronic transmission, storage, and retrieval provided that the electronic system provides for the maintenance of records as originally submitted without corruption, loss of data, or tampering.

(c) *Protection of SSI.* Each owner/operator must restrict the distribution, disclosure, and availability of security sensitive information, as identified in part 1520 of this chapter, to persons with a need to know. The owner/operator must refer requests for such information by other persons to TSA.

(d) *Availability.* Each owner/operator must make the records available to TSA upon request for inspection and copying.

Subpart C—Operations

§ 1570.201 Security Coordinator.

(a) Except as provided in paragraphs (b) and (c) of this section, each owner/operator identified in §§ 1580.1, 1582.1, and 1584.101 of this subchapter must designate and use a primary and at least one alternate Security Coordinator.

(b) An owner/operator identified in § 1582.1(a)(2) of this subchapter (public transportation agency) that owns or operates a bus-only operation must designate and use a primary and at least one alternate Security Coordinator only if the owner/operator is identified in appendix A to part 1582 of this subchapter or is notified by TSA in writing that a threat exists concerning that operation.

(c) An owner/operator identified in § 1580.1(a)(5) or § 1582.1(a)(4) of this subchapter (private rail car, tourist, scenic, historic, or excursion rail operations) must designate and use a primary and at least one alternate Security Coordinator, only if notified by TSA in writing that a threat exists concerning that type of operation.

(d) The Security Coordinator and alternate(s) must be appointed at the corporate level.

(e) Each owner/operator required to have a Security Coordinator must provide in writing to TSA the names, U.S. citizenship status, titles, phone number(s), and email address(es) of the Security Coordinator and alternate Security Coordinator(s) within 37 calendar days of the effective date of this rule, commencement of operations, or change in any of the information required by this section.

(f) Each owner/operator required to have a Security Coordinator must ensure that at least one Security Coordinator—

(1) Serves as the primary contact for intelligence information and security-related activities and communications with TSA. Any individual designated as a Security Coordinator may perform other duties in addition to the duties described in this section.

(2) Is accessible to TSA on a 24 hours a day, 7 days a week basis.

(3) Coordinates security practices and procedures internally and with appropriate law enforcement and emergency response agencies.

§ 1570.203 Reporting significant security concerns.

(a)(1) Except as provided in paragraph (a)(2) of this section, each owner/operator identified in §§ 1580.1, 1582.1, and 1584.101 of this subchapter must report, within 24 hours of initial discovery, any potential threats and significant security concerns involving transportation-related operations in the United States or transportation to, from, or within the United States as soon as possible by the methods prescribed by TSA.

(2) An owner/operator identified in § 1582.1(a)(2) of this subchapter (public transportation agency) that owns or operates a bus-only operation must only comply with the requirements in this section if the owner/operator is identified in appendix A to part 1582 of this subchapter or is notified by TSA in writing that a threat exists concerning that operation.

(b) Potential threats or significant security concerns encompass incidents, suspicious activities, and threat information including, but not limited to, the categories of reportable events listed in appendix A to this part.

(c) Information reported must include the following, as available and applicable:

(1) The name of the reporting individual and contact information, including a telephone number or email address.

(2) The affected freight or passenger train, transit vehicle, motor vehicle, station, terminal, rail hazardous materials facility, or other facility or infrastructure, including identifying information and current location.

(3) Scheduled origination and termination locations for the affected freight or passenger train, transit vehicle, or motor vehicle–including departure and destination city and route.

(4) Description of the threat, incident, or activity, including who has been notified and what action has been taken.

(5) The names, other available biographical data, and/or descriptions (including vehicle or license plate information) of individuals or motor vehicles known or suspected to be involved in the threat, incident, or activity.

(6) The source of any threat information.

[85 FR 16499, Mar. 23, 2020, as amended at 86 FR 23632, May 4, 2021]

Subpart D—Security Threat Assessments

§ 1570.301 Fraudulent use or manufacture; responsibilities of persons.

(a) No person may use or attempt to use a credential, security threat assessment, access control medium, or identification medium issued or conducted under this subchapter that was issued or conducted for another person.

(b) No person may make, produce, use or attempt to use a false or fraudulently created access control medium, identification medium or security threat assessment issued or conducted under this subchapter.

(c) No person may tamper or interfere with, compromise, modify, attempt to circumvent, or circumvent TWIC access control procedures.

(d) No person may cause or attempt to cause another person to violate paragraphs (a) through (c) of this section.

§ 1570.303 Inspection of credential.

(a) Each person who has been issued or possesses a TWIC must present the TWIC for inspection upon a request from TSA, the Coast Guard, or other authorized DHS representative; an authorized representative of the National Transportation Safety Board; or a Federal, State, or local law enforcement officer.

(b) Each person who has been issued or who possesses a TWIC must allow his or her TWIC to be read by a reader and must submit his or her reference biometric, such as a fingerprint, and any other required information, such as a PIN, to the reader, upon a request from TSA, the Coast Guard, other authorized DHS representative; or a Federal, State, or local law enforcement officer.

§ 1570.305 False statements regarding security background checks by public transportation agency or railroad carrier.

(a) *Scope.* This section implements sections 1414(e) (6 U.S.C. 1143) and 1522(e) (6 U.S.C. 1170) of the ''Implementing Recommendations of the 9/11 Commission Act of 2007,'' Public Law 110–53 (121 Stat. 266, Aug. 3, 2007).

(b) *Definitions.* In addition to the terms in §§ 1500.3, 1500.5, and 1503.202 of subchapter A and § 1570.3 of subchapter D of this chapter, the following term applies to this part:

Security background check means reviewing the following for the purpose of identifying individuals who may pose a threat to transportation security, national security, or of terrorism:

(i) Relevant criminal history databases.

(ii) In the case of an alien (as defined in sec. 101 of the Immigration and Nationality Act (8 U.S.C. 1101(a)(3)), the relevant databases to determine the status of the alien under the immigration laws of the United States.

(iii) Other relevant information or databases, as determined by the Secretary of Homeland Security.

(c) *Prohibitions.* (1) A public transportation agency or a contractor or subcontractor of a public transportation agency may not knowingly misrepresent to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary of Homeland Security related to security background check requirements for employees when conducting a security background check.

(2) A railroad carrier or a contractor or subcontractor of a railroad carrier may not knowingly misrepresent to an employee or other relevant person, including an arbiter involved in a labor arbitration, the scope, application, or meaning of any rules, regulations, directives, or guidance issued by the Secretary of Homeland Security related to security background check requirements for employees when conducting a security background check.

APPENDIX A TO PART 1570—REPORTING OF SIGNIFICANT SECURITY CONCERNS

Category	Description
Breach, Attempted Intrusion, and/or Interference.	Unauthorized personnel attempting to or actually entering a restricted area or secure site relating to a transportation facility or conveyance owned, operated, or used by an owner/operator subject to this part. This includes individuals entering or attempting to enter by impersonation of authorized personnel (for example, police/security, janitor, vehicle owner/operator). Activity that could interfere with the ability of employees to perform duties to the extent that security is threatened.
Misrepresentation	Presenting false, or misusing, insignia, documents, and/or identification, to misrepresent one's affiliation with an owner/operator subject to this part to cover possible illicit activity that may pose a risk to transportation security.
Theft, Loss, and/or Diversion	Stealing or diverting identification media or badges, uniforms, vehicles, keys, tools capable of compromising track integrity, portable derails, technology, or classified or sensitive security information documents which are proprietary to the facility or conveyance owned, operated, or used by an owner/operator subject to this part.
Sabotage, Tampering, and/or Vandalism	Damaging, manipulating, or defeating safety and security appliances in connection with a facility, infrastructure, conveyance, or routing mechanism, resulting in the compromised use or the temporary or permanent loss of use of the facility, infrastructure, conveyance or routing mechanism. Placing or attaching a foreign object to a rail car(s).

Category	Description
Cyber Attack	Compromising, or attempting to compromise or disrupt the information/technology infrastructure of an owner/operator subject to this part.
Expressed or Implied Threat	Communicating a spoken or written threat to damage or compromise a facility/infrastructure/conveyance owned, operated, or used by an owner/operator subject to this part (for example, a bomb threat or active shooter).
Eliciting Information	Questioning that may pose a risk to transportation or national security, such as asking one or more employees of an owner/operator subject to this part about particular facets of a facility's conveyance's purpose, operations, or security procedures.
Testing or Probing of Security	Deliberate interactions with employees of an owner/operator subject to this part or challenges to facilities or systems owned, operated, or used by an owner/operator subject to this part that reveal physical, personnel, or cyber security capabilities.
Photography	Taking photographs or video of facilities, conveyances, or infrastructure owned, operated, or used by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include taking photographs or video of infrequently used access points, personnel performing security functions (for example, patrols, badge/vehicle checking), or security-related equipment (for example, perimeter fencing, security cameras).
Observation or Surveillance	Demonstrating unusual interest in facilities or loitering near conveyances, railcar routing appliances or any potentially critical infrastructure owned or operated by an owner/operator subject to this part in a manner that may pose a risk to transportation or national security. Examples include observation through binoculars, taking notes, or attempting to measure distances.
Materials Acquisition and/or Storage	Acquisition and/or storage by an employee of an owner/operator subject to this part of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and/or timers that may pose a risk to transportation or national security (for example, storage of chemicals not needed by an employee for the performance of his or her job duties).
Weapons Discovery, Discharge, or Seizure..	Weapons or explosives in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that may present a risk to transportation or national security (for example, discovery of weapons inconsistent with the type or quantity traditionally used by company security personnel).
Suspicious Items or Activity	Discovery or observation of suspicious items, activity or behavior in or around a facility, conveyance, or infrastructure of an owner/operator subject to this part that results in the disruption or termination of operations (for example, halting the operation of a conveyance while law enforcement personnel investigate a suspicious bag, briefcase, or package).

PART 1572—CREDENTIALING AND SECURITY THREAT ASSESSMENTS

Subpart A—Procedures and General Standards

Sec.

Subpart B—Qualification Standards for Security Threat Assessments

Subpart C—Transportation of Hazardous Materials From Canada or Mexico To and Within the United States by Land Modes

Subpart D [Reserved]