DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Parts 1500, 1520, 1570, 1580, 1582, and 1584

[Docket No. TSA–2015–0001]

RIN 1652–AA55

Security Training for Surface Transportation Employees

AGENCY: Transportation Security Administration, DHS.

ACTION: Final rule.

SUMMARY: The Transportation Security Administration (TSA) is requiring owner/operators of higher-risk freight railroad carriers, public transportation agencies (including rail mass transit and bus systems), passenger railroad carriers, and over-the-road bus companies, to provide TSA-approved security training to employees performing security-sensitive functions. The training curriculum must teach employees how to observe, assess, and respond to terrorist-related threats and/or incidents. Additionally, TSA is expanding its requirements for security coordinators and reporting of significant security concerns (currently limited to rail operations) to include bus operations within the scope of the regulation's applicability. TSA is amending other provisions of its regulations, as necessary, to implement these requirements.

DATES:

Effective date: This rule is effective June 22, 2020.

Compliance date: In general, compliance schedules are indicated in this rule. The requirements in 49 CFR 1570.201 must be met no later than July 29, 2020.

FOR FURTHER INFORMATION CONTACT: Harry Schultz (TSA, Security Policy and Industry Engagement, Surface Division) or David Kasminoff (TSA, Senior Counsel, Regulations and Security Standards) at telephone (571) 227–5563, or email to *SecurityTrainingPolicy@tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

Availability of Rulemaking Document

An electronic copy can be obtained using the internet by—

(1) Searching the electronic Federal Docket Management System (FDMS) web page at *http://www.regulations.gov;*

(2) Accessing the Government Printing Office's web page at *http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=FR* to view the daily published **Federal Register** edition; or accessing the ''Search the Federal Register by Citation'' in the ''Related Resources'' column on the left, if you need to do a Simple or Advanced search for information, such as a type of document that crosses multiple agencies or dates.

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires TSA to comply with small entity requests for information and advice about compliance with statutes and regulations within TSA's jurisdiction.[1] Any small entity that has a question regarding this document may contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section. Persons can obtain further information regarding SBREFA on the Small Business Administration's web page at *https://www.sba.gov/category/advocacy-navigation-structure/regulatory-policy/regulatory-flexibility-act/sbrefa.*

Abbreviations and Terms Used in This Document

Amtrak—National Railroad Passenger Corporation
APTA—American Public Transportation Association
CDL—Commercial Driver's License
DHS—Department of Homeland Security
DOT—Department of Transportation
FRA—Federal Railroad Administration
FTA—Federal Transit Administration
GAO—U.S. Government Accountability Office
HSA—Homeland Security Act of 2002
HTUA—High Threat Urban Area
IED—Improvised Explosive Device
MOU—Memorandum of Understanding
NSI—Nationwide Suspicious Activity Reporting (SAR) Initiative
OMB—Office of Management and Budget
OSHA—Occupational Health and Safety Administration
OTRB—Over-the-Road Bus
PHMSA—Pipeline and Hazardous Materials Safety Administration
PRA—Paperwork Reduction Act of 1995
PTPR—Public Transportation and Passenger Railroads
RFA—Regulatory Flexibility Act of 1980
RIA—Regulatory Impact Analysis
RSC—Rail Security Coordinator
RSSM—Rail Security-Sensitive Material
SBA—Small Business Administration
SBREFA—Small Business Regulatory Enforcement Fairness Act of 1996
SSI—Sensitive Security Information
TSA—Transportation Security Administration
TSSM—Transportation Security-Sensitive Material
UASI—Urban Area Security Initiative
UMRA—Unfunded Mandates Reform Act of 1995
VBIED—Vehicle-Borne Improvised Explosive Device

Table of Contents

[1] Public Law 104–121, 110 Stat. 857 (Mar. 29, 1996).

I. Executive Summary and Background

A. Statutory Mandate

Following the attacks of September 11, 2001, Congress created TSA under the Aviation and Transportation Security Act (ATSA) and established the agency's primary Federal role to enhance security for all modes of transportation.[2] The scope of TSA's authority includes assessing security risks, developing security measures to address identified risks, and enforcing compliance with these measures.[3] TSA also has broad regulatory authority to issue, rescind, and revise regulations as necessary to carry out its transportation security functions.[4]

As part of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act),[5] Congress mandated regulations to enhance surface transportation security through security training of frontline employees. The mandate includes prescriptive requirements for who must be trained, what the training must encompass, and how to submit and obtain approval for a training program.[6] The 9/11 Act also mandates regulations requiring higher-risk railroads and over-the-road buses (OTRBs) to appoint security coordinators.[7] In addition to implementing these provisions, this final rule also addresses a mandate to define Transportation Security-Sensitive Materials.[8]

B. Benefits of Requiring Security Training

TSA is issuing this rule pursuant to its authority and responsibility over the security of the nation's transportation systems. TSA fulfills its transportation security mission in partnership with its industry and government stakeholders. As noted in the 2018 *National Strategy for Counterterrorism in the United States:*

> The critical infrastructure of the United States—much of which is privately owned—provides the essential goods and services that drive American prosperity. Coordinated efforts are, therefore, necessary to strengthen and maintain secure and resilient critical infrastructure and to prepare Americans to respond appropriately should an attack occur. By integrating and improving preparedness across all levels of government as well as the private and public sectors, we will stop terrorists from undermining our security and prosperity.[9]

Consistent with this strategy, the purpose of this rule is to solidify the baseline of security for higher-risk surface transportation operations by improving and sustaining the preparedness of surface transportation employees in higher-risk operations, including their critical capability to observe, assess, and respond to security risks and potential security breaches within their unique working environment. In developing this rulemaking, TSA recognizes private sector capabilities, voluntary initiatives, and other Federal requirements to raise security within distinct surface transportation operations. By integrating these efforts, setting a national standard for surface transportation employee security training, and ensuring this training is sustained across higher-risk operations, this rule promotes national security in alignment with the intent of the 9/11 Act and the *National Strategy.*

The rule accomplishes this purpose by requiring higher-risk public transportation systems, railroad carriers (passenger and freight), and OTRB owner/operators to prepare and train their employees performing security-sensitive job functions. Through security training, employees will have the capability to identify, report, and appropriately react to suspicious activity, suspicious items, dangerous substances, and security incidents that may be associated with terrorist reconnaissance, preparation, or action. TSA believes this training may be the critical point for preventing a terrorist act and mitigating the consequences.

In order to ensure effective communication regarding threats (both to regulated parties and from regulated parties), TSA is also expanding applicability of current requirements for rail operations to have security coordinators and report security incidents to TSA. With this rulemaking,

[2] Public Law 107–71, 115 Stat. 597 (Nov. 19, 2001). ATSA created TSA as a component of the Department of Transportation (DOT). Section 403(2) of the Homeland Security Act of 2002 (HSA), Public Law 107–296, 116 Stat. 2135 (Nov. 25, 2002), transferred all functions related to transportation security, including those of the Secretary of Transportation and the Under Secretary of Transportation for Security, to the Secretary of Homeland Security. Pursuant to DHS Delegation Number 7060.2, the Secretary delegated to the Administrator, subject to the Secretary's guidance and control, the authority vested in the Secretary with respect to TSA, including the authority in sec. 403(2) of the HSA.

[3] *See* 49 U.S.C. 114, which codified section 101 of ATSA.

[4] 49 U.S.C. 114(l)(1).

[5] Public Law 110–53, 121 Stat. 266 (Aug. 3, 2007).

[6] *See* secs. 1408, 1517, and 1534 of the 9/11 Act, codified at 6 U.S.C. 1137, 1167, and 1184, respectively.

[7] *See* secs. 1512 and 1531 of the 9/11 Act, codified at 6 U.S.C. 1162 and 1181, respectively. TSA addresses 1512(e)(1)(A) and 1531(e)(1)(A) in this rulemaking. TSA intends to address the other regulatory requirements of these provisions in separate rulemakings.

[8] *See* sec. 1501 of the 9/11 Act, codified at 6 U.S.C. 1151.

[9] *See* The White House, *National Strategy for Counterterorrism in the United States,* at 19 (Oct. 2018), available at *https://www.dni.gov/files/NCTC/documents/news_documents/NSCT.pdf* (last accessed Nov. 26, 2018) (*National Strategy*).

the applicability for this requirement is expanded to include any owner/operator required to provide security training. Requiring higher-risk owner/operators to have security coordinators and report significant security concerns to TSA will enhance TSA's ability to recognize trends and communicate directly with individuals within higher-risk operations that have direct responsibility for security.

C. Costs of This Final Rule

Table 1 identifies TSA's estimates for the overall cost of this rule.

TABLE 1—COST OF FINAL RULE

	Estimated costs (over 10 years, discounted at 7 percent)
Freight Railroads	$25.09 million.
Public Transportation and Passenger Railroads (PTPRs).	17.12 million.
OTRBs	8.06 million.
TSA	2.03 million.
Total	52.30 million.

D. Organization of This Final Rule

Subchapter D of chapter XII of title 49, ''Maritime and Surface Transportation Security'' [10] (Subchapter D), includes security program requirements for surface transportation, including the requirements in this final rule. Before this final rule, Subchapter D included requirements relevant to two vetting programs (the Transportation Worker Identification Credential (TWIC) and Hazmat Material Endorsement (HME), as well as certain rail security requirements, including chain of custody for Rail Security-Sensitive Materials (RSSM), appointment of security coordinators, and reporting security issues.

This final rule (1) adds requirements for security training for certain surface transportation owner/operators; (2) expands applicability of the security coordinator and reporting security issue requirements to include higher-risk bus operations; and (3) adds other miscellaneous provisions necessary for implementation of a new regulatory program.

To incorporate these new elements, TSA is organizing Subchapter D as follows.

- Part 1570 is divided into four subparts: (1) Subpart A includes requirements generally applicable to all aspects of subchapter D; (2) subpart B includes security program requirements consistently relevant to multiple modes; (3) subpart C includes operational requirements consistently applicable to multiple modes; and (4) subpart D moves and consolidates general provisions related to security threat assessments (STAs) which are more specifically addressed in part 1572. As noted below, mode-specific requirements are contained in subsequent parts.
- Part 1580 is modified to limit requirements applicable to rail security. This part includes operational requirements unique to freight railroads and rail hazardous materials shippers/receivers (such as chain of custody) [11] and modal-specific security training requirements for freight railroads. The requirements for appointment of security coordinators and reporting security issues are moved to part 1570 and several definitions are moved to part 1500.
- Part 1582, a new part entitled ''Public Transportation and Passenger Railroad Security,'' includes modal-specific security training requirements for public transportation system and passenger railroads (PTPR). The requirements for appointment of security coordinators and reporting security issues applicable to PTPR rail operations are moved to part 1570 and several definitions are moved to part 1500.
- Part 1584, a new part entitled, ''Highway and Motor Carrier Security,'' includes modal-specific security training requirements for OTRB owner/operators.

Owner/operators subject to the requirements of this final rule will need to address the requirements in part 1570 as well as the requirements applicable to their respective mode in parts 1582 through 1584. Sections II through IV, which follow, provide a comprehensive discussion of these requirements as they will be implemented, rather than a sequential section-by-section analysis. Section II addresses general programmatic requirements, including: Applicability determinations, which employees must be trained, content of training, and the required training schedule. Section III discusses operational requirements, such as the requirement for security coordinators and reporting of security incidents. Section IV provides the procedural requirements for submission and approval of a security training program, amendments to the program, and recordkeeping requirements. This section also includes a table that summarizes the compliance deadlines owner/operators must meet. Section V discusses other revisions to TSA's regulations that result from adding these new requirements to Subchapter D.[12]

This final rule includes TSA's responses to comments received on the NPRM. Section VI includes a chart summarizing the minimal changes between the NPRM and final rule. Section VII provides TSA's responses to comments on the NPRM.

Section VIII includes the rulemaking analysis and notices. This analysis includes any changes in the impact estimates between the NPRM and the final rule and the basis for those changes.

II. Security Program Requirements

A. Who must provide security training?

Consistent with TSA's commitment to a risk-based approach to transportation security, the requirements of this rule only apply to higher-risk operations. A higher-risk operation is one that meets the criteria in §§ 1580.101 (freight railroads), 1582.101 (PTPR), and 1584.101 (OTRB). These criteria are used to identify operations with a relatively higher-risk of being targeted or used by terrorists. While there are approximately 10,000 surface transportation operations, approximately 300 of them currently meet the criteria.[13]

While the requirements of this rule are limited to higher-risk operations, TSA encourages all owner/operators to consider implementing the security training program required by this rule, modified and adapted to their operations, as appropriate. TSA will ensure resources developed for regulated owner/operators, such as TSA-created training materials, are available to owner/operators of non-higher-risk operations who are committed to enhancing security through improving the security awareness of employees.

TSA's applicability criteria for freight railroads, PTPR, OTRB, and certain business operations are as follows.

1. Freight Railroads (§ 1580.101)

A freight railroad owner/operator must provide security training if it is: (a)

[10] TSA is modifying the title of this subchapter, changing it from ''Maritime and Land Transportation Security'' to ''Maritime and Surface Transportation Security.''

[11] *See* Rail Transportation Security Final Rule (Rail Security Rule), 73 FR 72130, (Nov. 26, 2008).

[12] The discussion does not address provisions that are moved, as discussed above, but not modified.

[13] A full discussion of TSA's analysis and considerations in making its determination and developing the applicability criteria can be found in the NPRM. *See* 81 FR at 91355 *et seq.* (section III.F. of the NPRM).

Designated as Class I; [14] (b) transports RSSM in one or more of the areas listed in current Appendix A to 49 CFR part 1580; [15] and/or (c) hosts a higher-risk rail operation (including freight railroads and the intercity or commuter systems identified in § 1582.101). The flowchart in Figure 1 summarizes when a freight railroad owner/operator must provide security training and when this training is recommended by TSA. TSA estimates the requirements of this rule currently apply to 33 freight railroads.

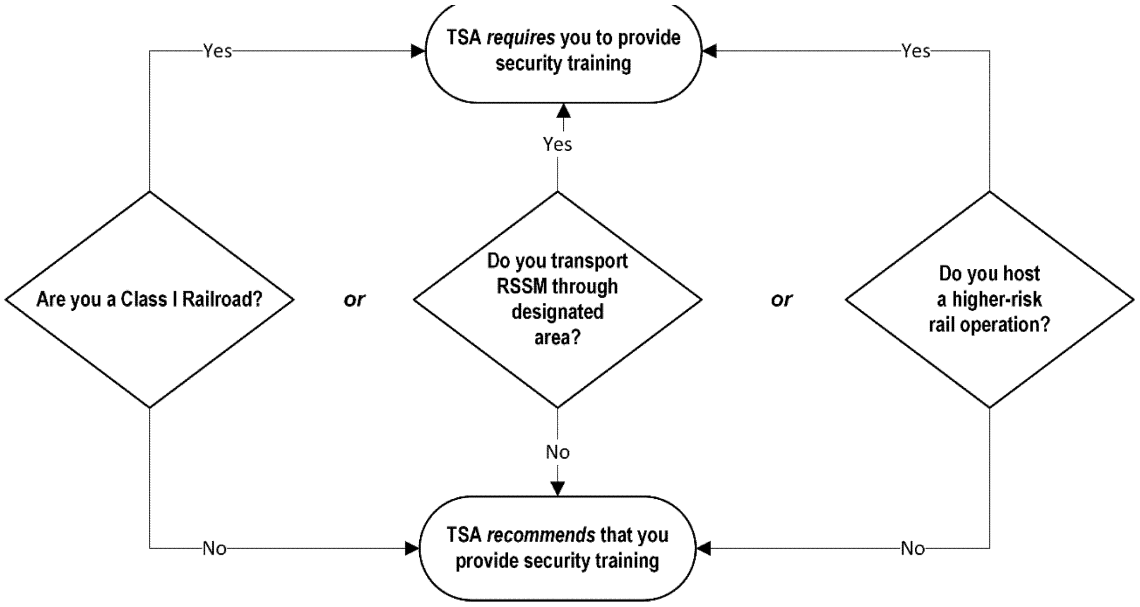

Figure 1. Freight Railroad Applicability Flow Chart

2. Public Transportation and Passenger Railroads (§ 1582.101)

A public transportation agency or passenger railroad must provide security training if it is (a) one of the 46 identified PTPR systems listed in 49 CFR part 1582, Appendix A; (b) Amtrak; or (c) hosts a higher-risk freight railroad. DHS consistently identifies the eight regions where the 46 systems operate as having the highest transit-specific risk. Applying the rule's requirements to these systems corresponds to providing enhanced security for more than 80 percent of all PTPR passengers.

3. Over-the-Road Buses (§ 1584.101)

An OTRB owner/operator must provide security training if it provides fixed-route service to, through, or from any of ten areas identified in 49 CFR part 1584, Appendix A. These ten areas receive the highest funding allocation under the FY 2018 Urban Area Security Initiative (UASI) grant program (87 percent of the total available funding).[16] TSA estimates that this rule will apply to approximately 205 OTRB owner/operators.

The determining factor for whether a fixed-route OTRB owner/operator is within the scope of the rule is not where they are headquartered, but where they provide service. In deciding to rely on where the owner/operator provides service, rather than corporate headquarters locations, TSA considered factors that could make an OTRB a potential target for a terrorist attack, including (1) its visibility (the size of its operations); (2) the extent to which its schedule is publicly available; (3) whether or not it is relatively easy for unknown individuals to board the bus; (4) and whether the bus will have ease of access to high-consequence locations.

TSA is aware that some private companies provide commuter services that may trigger applicability of the rule. Figure 2 provides a flowchart to assist companies with determining if the security training requirements apply.

[14] The Surface Transportation Board defines a Class I railroad as one with annual operating revenue in excess of $447,621,226 (adjusted for inflation).

[15] *See* § 1580.3 for definition of RSSM.

[16] UASI funds are allocated based on a risk methodology employed by DHS and the Federal Emergency Management Agency (FEMA). For the list of UASI allocations for the FY 2018 UASI grant program, which is administered by FEMA as part of the larger Homeland Security Grant Program, see the FY 2018 Homeland Security Grant Program Notice of Funding Opportunity, Appendix A at *https://www.fema.gov/media-library-data/1526578809767-7f08f471f36d22b2c0d8afb848048c96/FY_2018_HSGP_NOFO_FINAL_508.pdf.*

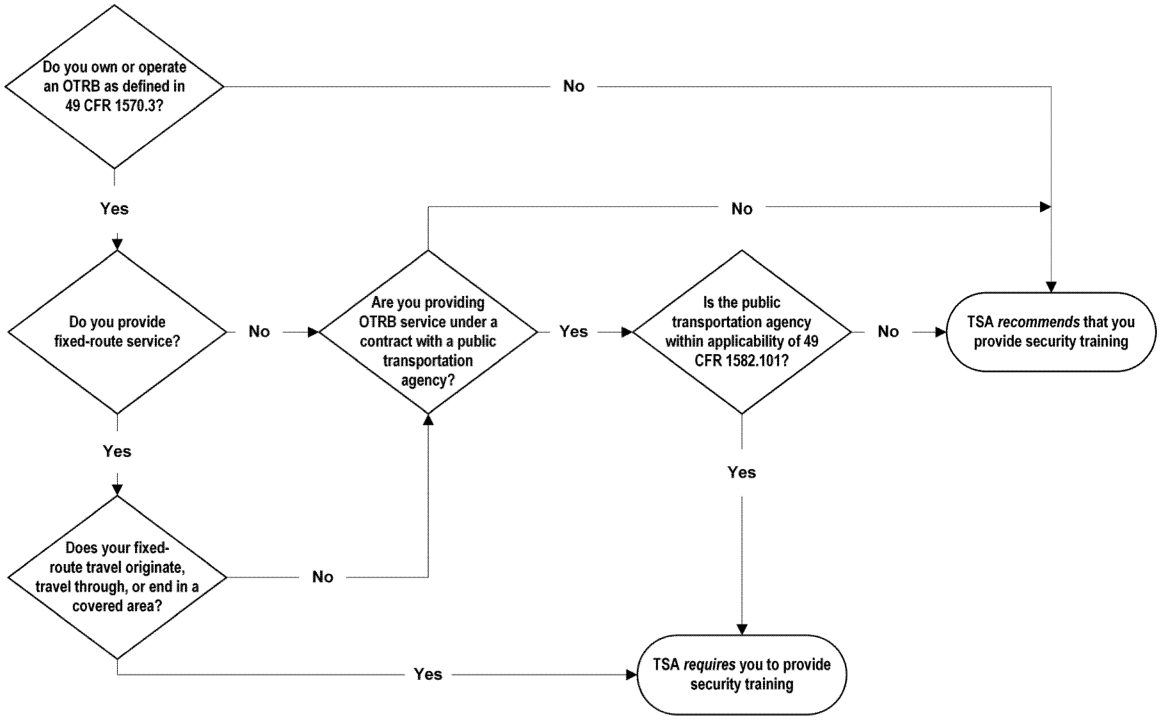

Figure 2. Commuter Bus Service Applicability Flowchart

4. Impact on Certain Business Operations

Parent corporations and subsidiaries. While the criteria for higher-risk determinations presumes similarities for operations within each mode,[17] TSA recognizes there are other considerations that could affect applicability, particularly related to subsidiaries. As discussed in section III.F of the NPRM,[18] TSA is limiting the requirements to the level of the subsidiary whose operations fit the applicability criteria identified in the rule.

During the review and approval process of the security training program, TSA will work with owner/operators to address any compliance issues based on corporate structure. For example, owner/operator A may be organized to make each regional area a separate subsidiary. As such, only the subsidiary that meets the applicability requirements must develop a security training program. Owner/operator B may be a single entity for purposes of corporate-legal structure with branches, rather than subsidiaries, providing service on specific routes. Under this rule, the entire corporation is subject to the requirements based on the operations of one route. In this situation, owner/operator B could choose to submit a proposed alternative to limit application of the requirements to branches and a handful of headquarters or other regional employees that provide operational support. The submission requirements and procedures for requesting alternative measures are discussed in section IV.

Foreign owner/operators. While the applicability provisions for security training do not specifically reference foreign owner/operators, the requirements apply to employees performing a security-sensitive function ''. . . in the United States or in direct support of the common carriage of persons or property between a place in the United States and any place outside the United States.'' Therefore, the training requirements of this rule apply to both domestic owner/operators and foreign owner/operators with employees performing covered functions within the United States or in support of operations within the United States. For example, the rule may apply to a Canadian OTRB owner/operator offering fixed-route service that begins at a point in Canada and transits through an area identified in part 1584, Appendix A before concluding at a point in Mexico. Even if only one employee (for example, the driver), performs a security-sensitive function while physically in the United States, applicability is triggered by the route. The Canadian OTRB owner/operator would be required to have a security training program and provide the required training to the driver and any other employee performing a security-sensitive function that supports the operations transiting through higher-risk regions in the United States (such as individuals providing maintenance or inspection services and dispatch information applicable to the covered route). Once applicability is triggered, it is irrelevant where the OTRB owner/operator's company is located or where the function is being performed (whether the employee is performing the security-sensitive function at a location in Canada or along the route in the United States).

In addition, while foreign owner/operators providing service in the United States are required to have a security coordinator and alternate, foreign owner/operators are only required to report potential threats and significant security concerns for operations in the United States or transportation to, from, or within the United States. A similar requirement currently applies to foreign freight railroad owner/operators under 49 CFR part 1580. This approach is also consistent with that taken by the Federal Railroad Administration (FRA).

Hosting relationships. TSA recognizes that joint operations are common within the rail industry and include agreements

[17] *See* discussion on applicability at 81 FR 91355 *et seq.* (sec. III.F. of NPRM).

[18] 81 FR at 91355.

such as hosting. In a hosting relationship, the ''host railroad'' owns the track and exercises operational control of the movement of trains of other railroads (the ''tenant'' railroads) while they are using that track.

Under this rule, both the host and tenant railroads are required to have a training program that appropriately addresses the ramifications of the hosting relationship. For example, the host railroad's training program will need to address the operational considerations of the hosting relationship, such as training dispatchers on their role and responsibilities in halting the tenant railroad's operations over a segment of track where there is a potential threat (such as a suspected improvised explosive device (IED) or tampering with infrastructure). Similarly, a tenant railroad subject to the security training requirements of 49 CFR part 1582 (PTPR), will need to address the operational considerations of the hosting relationship, such as instructing its train and engine employees on the proper communication procedures to follow when a potential threat is identified. Under either example, the host and tenant railroad owner/operators are only responsible for training their own employees.

Contracted services. Contracted services may involve joint operation pursuant to specific terms, but are different from hosting relationships. For example, some commuter passenger train services are owned by public transportation agencies, but the agency has a contract with a private company (such as a freight railroad) to operate the train. This is not a hosting relationship.

When inspecting compliance by participants in this type of a contracted services agreement, TSA will consider the freight railroad carrier (the private company/contractor) to be an authorized representative of the PTPR owner/operator (the owner/operator of the passenger train service). TSA will hold the PTPR owner/operator primarily responsible for compliance and for ensuring that all security-sensitive employees receive the required training, whether they are employed directly by the PTPR owner/operator or contractor. The PTPR owner/operator must train the freight railroad carrier's employees performing security-sensitive functions related to the passenger train service.

To the extent the contract between the PTPR owner/operator and the freight railroad includes a provision for the freight railroad to train its own employees, the passenger operation is responsible for documenting satisfaction of the training requirements within its TSA-approved-security training program. TSA will expect the passenger operation to clearly state in its security training program, as part of the submission process under 49 CFR 1570.109, that the freight railroad carrier will conduct the training and provide the required information on that training.

Regardless of how the parties define who will do what, TSA has authority to inspect both parties' operations for compliance. The regulated party is primarily responsible, but TSA has authority to initiate enforcement actions for non-compliance against either party based upon a fact-specific determination. While TSA historically initiates enforcement actions against the regulated entity, we have begun to look more closely at authorized representative/contractual relationships in our effort to address the root cause of noncompliance.

B. Who is responsible for determining whether a specific owner/operator is subject to the requirements of the rule (applicability determinations)? (§ 1570.105)

Owner/operators are required to use the criteria in 49 CFR parts 1580, 1582, and 1584 (contained in a subpart B to each part) to determine whether their operations are higher-risk. If the operations meet the criteria, the requirements of this rule apply. Under § 1570.105(a), owner/operators must notify TSA within 30 days of the effective date of this final rule if they meet the criteria for applicability. This obligation also applies to new and modified operations (commencing after publication of the final rule). Under § 1570.105(b), owner/operators must notify TSA no later than 90 calendar days before commencing operations or implementing modifications triggering applicability of the requirements.

While the rule requires owner/operators to determine whether the criteria apply, TSA is aware of the operations that are likely to be within the scope of applicability. TSA may initiate a compliance investigation if an owner/operator fails to self-identify within the required period.

To mitigate the likelihood of an owner/operator failing to comply based upon lack of recognition of the applicability for these requirements, TSA will use a variety of communication strategies to notify regulated parties that are likely to meet the applicability criteria. For example, TSA will use email to immediately notify its key stakeholder points of contact regarding publication of this final rule. In addition to these established information sharing mechanisms, TSA also conducts regular calls, workshops, and meetings with major industry partners and trade associations. TSA's surface representatives also work closely with surface-system owner/operators during industry-led security work groups, conferences, roundtables, and other sector-specific government coordination meetings. TSA plans to use all of these mechanisms to notify relevant industry partners of the new requirements.

C. Which employees must receive security training? (§§ 1580.115(a), 1582.115(a) and 1584.115(a))

Any owner/operator required to have a security training program under §§ 1580.101, 1582.101, or 1584.101, must provide security training to all security-sensitive employees. Security-sensitive employees include any direct employee, contractor, employee of a contractor, or other authorized person who is compensated for performing a security-sensitive function on behalf of or for the benefit of the owner/operator.[19] For example, if an OTRB owner/operator does not employ any drivers directly, but uses drivers under contract, these drivers will need to be trained. Similarly, if an owner/operator has chosen to combine dispatch services with any affiliates of its parent corporation, the owner/operator required to provide security training to its direct employees will also be required to provide security training to any dispatchers providing services for its fleet.

D. How does an owner/operator determine if someone is a security-sensitive employee? (§§ 1580.3, 1582.3, and 1584.3)

Definitions of mode-specific ''security-sensitive employees'' are included in §§ 1580.3 (freight rail), 1582.3 (PTPR), and 1584.3 (OTRB), with additional detail regarding job functions provided in mode-specific tables published as appendices to parts 1580,[20] 1582, and 1584. As discussed in section III.E. of the NPRM, ''security-sensitive employees'' are individuals who perform functions with a direct nexus to, or impact on, transportation

[19] *See* § 1570.3 for the definition of an ''employee.''

[20] The table in part 1580 Appendix B is unique in that it includes examples of the job titles related to these functions based on historic use of these terms for railroads. The job titles, however, are provided solely as a resource to help understand the functions described; whether an employee must be trained is based upon the function, not the job title.

security.[21] These functions fall into the following categories: (1) Operating a vehicle; inspecting and maintaining vehicles; (2) inspecting or maintaining building or transportation infrastructure; (3) controlling dispatch or movement of vehicles; (4) providing security of the owner/operator's equipment and property; (5) loading or unloading cargo or baggage; (6) interacting with travelling public (on board a vehicle or within a transportation facility); and (7) complying with security programs or measures, including those required by Federal law (a catch-all category that includes a small number of employees such as security coordinators and any other individuals who may have responsibility for carrying out aspects of the owner/operator's security program or other security measures who are not otherwise identified in the previous categories).

The requirements also apply to managers, supervisors, or others who perform a security-sensitive function or who so directly supervise the performance of such a function that their nexus is equivalent to the security-sensitive employee.[22] For example, a yardmaster in freight railroad operations is considered a security-sensitive employee because he or she directs security-sensitive functions, even if not in the direct management chain of all individuals performing these functions. At the same time, individuals within a corporate structure who neither perform a security-sensitive function nor have direct management responsibilities over individuals who do are unlikely to have a position within the corporation with a significant nexus to the transportation operations of the business (such as accounting functions). To the extent there are such individuals in the management structure, they will not be considered ''security-sensitive'' employees.

In some circumstances, security-sensitive functions may be performed by individuals not within the definition of ''employee.'' For example, police officers employed by a local law enforcement agency may be routinely patrolling the owner/operator's premises and/or operations, but do not work directly for, or under contract to, the owner/operator. Owner/operators are not required to provide training to these individuals. To the extent, however, these individuals work in the same environment as security-sensitive employees, TSA encourages owner/operators to make their training materials and sessions available. Providing awareness of training content to local law enforcement personnel regularly assigned to patrols at locations where security-sensitive employees work can enhance communication and cooperation in response to potential threats or actual terrorist-related incidents.

The law enforcement agency or personnel may be considered security-sensitive employees of the owner/operator if, for example, there is a contractual relationship for the law enforcement agency to provide services to the owner/operator and the law enforcement officer is assigned to that location by the owner/operator. Similarly, where the owner/operator has a dedicated police or security force who are employees of the owner/operator, these individuals are security-sensitive employees who must be trained under this rule.

TSA encourages owner/operators to consider other employees within their corporate structure or business operations who may not be performing a security-sensitive function as identified in the rule, but who could provide an additional layer of security if they received security training. Furthermore, if an owner/operator identifies positions or functions not listed by TSA as security-sensitive, but which have the nexus to transportation security that is intended to be covered by the rule, TSA encourages the owner/operator to identify and include these employees within its security training program.

E. Can untrained security-sensitive employees perform security-sensitive functions? (§§ 1580.115(b), 1582.115(b), and 1584.115(b))

If a security-sensitive employee does not receive the required security training, this employee is prohibited from performing a security-sensitive function without the direct supervision of an employee who has met the training requirements applicable to that security-sensitive function. While TSA is not defining ''direct,'' TSA expects the supervisor to be located in reasonable proximity to the employee to supervise actions and provide the necessary level of security awareness and response capabilities.

Furthermore, even if an employee is directly supervised, TSA imposes a 60-day limit for the amount of time that an employee may perform a security-sensitive function without completing the required training. After 60 days, the rule requires the owner/operator to remove the employee from a security-sensitive function. This requirement does not affect the owner/operators' discretion to reassign the individual to other non-security-sensitive job functions.

F. What topics must be included in the security training? (§§ 1580.115(c)–(f), 1582.115(c)–(f), and 1584.115(c)–(f))

TSA is requiring a training program that focuses on the specific knowledge provided to security-sensitive employees related to preparedness, observation, assessment and response. As a key aspect of security awareness is the ability to detect anomalies in the operating environment, the rule affords flexibility for owner/operators to develop and implement a program that addresses the above-required components in the context of their unique operational environments.

The ''prepare'' category addresses training on discharging any security responsibilities that security-sensitive employees may have under an owner/operator's existing security plan or security measure. This rule does not require any owner/operator to adopt or implement a security plan or measures, but TSA is aware that many owner/operators have security plans or measures implemented to comply with Federal requirements, to qualify for Federal grants, or as the result of voluntary initiatives. To the extent these plans or procedures exist, employees must be trained in order to ensure they are effective. Similar to the threat and incident prevention and response training, this portion of the training program will need to be tailored to the specific operation.

The ''prepare'' element provides multiple benefits to transportation security and to owner/operators. First, the requirement recognizes that the time when a crisis is occurring is not the time to provide training on how to implement crisis-response measures. Employees need to be prepared in advance, especially if they have responsibilities related to responding to a terrorist incident in order to mitigate the consequences. Second, this training element ensures that training conducted under this rule meets all of the requirements for security training required for ''hazmat employees'' under 49 CFR 172.704(a)(5).[23] Third, this

[21] *See* 81 FR at 91353 *et seq.* for more information on how TSA identifies these employees and how the chosen functions align with requirements in the 9/11 Act.

[22] The definition of ''employee,'' which is in § 1570.3, includes immediate supervisors.

[23] An analysis of the relationship between the Pipeline and Hazardous Materials Safety Administration (PHMSA) required training and the training provided by this final rule can be found in Diagram B of the NPRM. *See* 81 FR at 91364. The relation with other training is also discussed in section II.H. and I. of this preamble.

element also captures specific training for freight railroads related to the requirements in § 1580.115(c) for chain of custody and control requirements, ensuring appropriate procedures are followed to comply with the security requirements in subpart C to part 1580 (which contains the requirements moved from §§ 1580.103 and 1580.107 as a result of this rulemaking).

Finally, the ''prepare'' category captures training that may vary based on the specific nature of an employee's responsibilities. For example, appropriate methods of self-defense may vary based upon an employee's job and extent to which he or she interacts with the public. Similarly, an employee's need to be trained in how to operate and maintain security equipment may be dictated by the employee's responsibilities. Within this category, owner/operators have some flexibility to shape the training to be appropriate for their specific employees and operations. This flexibility allows owner/operators to avoid situations where employees are required to sit through training completely irrelevant to their roles and responsibilities.

TSA intends for the training required in the Observe, Assess, and Respond categories to be relevant to all employees, regardless of their job functions. Training in security awareness and behavior recognition is appropriate for all employees and TSA believes there should be a common level of proficiency on these issues among security-sensitive employees of the owner/operators.

The ''observe'' category is intended to provide knowledge to increase a security-sensitive employee's observational skills. In general, this training focuses on recognizing the difference between what is normal for the operational environment and abnormalities that could indicate terrorist planning or imminent attack. Training delivered should teach the employees that suspicious activity is a combination of actions and individual behaviors that appear strange, inconsistent, or out of the ordinary for the employee's work environment. In most instances, it will not be a single factor, but a combination of factors taking place at a particular time and place, that will accurately identify a suspicious individual or act.

The ''assess'' category requires providing knowledge of how to determine the most appropriate response to what is observed. For example, does the incident require a response and, if so, what is the appropriate response?

The ''respond'' category includes training on security incident responses—including how to appropriately report a security threat, interact with the public and first responders at the scene of a threat or incident, applicable uses of self-defense devices or protective equipment, and communication with passengers. In addition to meeting training requirements enumerated in the 9/11 Act,[24] this category is intended to provide elements of security awareness training required by 49 CFR 172.704(a)(4). To the extent owner/operators need to provide training on specific self-defense devices or protective equipment, TSA has not calculated these costs. Such training is not a cost of this rule based on an assumption that training on the use of self-defense devices and equipment is a standard part of any operation before providing such devices or equipment to individuals.

TSA recognizes that owner/operators may choose, or have chosen, to integrate varying levels of training into their security training programs, such as for particular categories of employees or job functions, to meet the objectives of their overall security program or plan. As noted in section I, TSA intends for this rule to establish and solidify the baseline of security for higher-risk surface transportation operations. To the extent an owner/operator has a program that goes beyond the required baseline, TSA encourages continuation of these efforts as long as the owner/operator can meet the minimum training required by this rule for all security-sensitive employees.

G. Who will provide the security training curriculum? (§§ 1580.113, 1582.113, and 1584.113)?

Owner/operators are required to train security-sensitive employees using curriculum approved by TSA. TSA assumes that many of the owner/operators required to provide security training under this rule already have training programs in place that may substantially comply with the rule's requirements. This assumption is based on TSA's involvement in allocations of grant funding to owner/operators for the development of security training materials, funded through various DHS-grant program appropriations, as well as a comprehensive review of available training materials to determine whether they meet the standards and criteria required by the 9/11 Act. This assumption is also bolstered by certain industry responses to TSA's Notice published in 2013 in which TSA sought public comment and data on current security training practices.[25]

TSA is committed to mitigating the costs of training for all owner/operators through several initiatives. For example, TSA has, and will continue, to identify existing training materials that address the curriculum content requirements identified in the rule and will make this information available to regulated parties.[26] TSA is also developing training materials that meet specific training requirements in this rule. TSA will notify regulated parties as the relevant training materials are completed.

H. Can owner/operators use pre-existing material or other third-party material? (§ 1570.103)

This rule does not require the owner/operator to create their own material or impose limits on the use of third-party material. If, however, owner/operators choose to rely on previously prepared training material, including material developed to satisfy other regulatory requirements, or third-party material, they must incorporate that material into an appendix to their security training program and reference that appendix in the corresponding portions of their security program, as discussed below.

I. How do these requirements relate to other security training required by other Federal or State agencies? (§§ 1580.115(c), 1582.115(c), and 1584.115(c))

TSA recognizes that many owner/operators covered by this rule are subject to training requirements under regulations of the Department of Transportation (DOT) that overlap with the training content required in the 9/11 Act.[27] TSA does not expect owner/operators to duplicate training. To the extent that an owner/operator intends to use existing training programs

[24] Diagram B in the NPRM, *Development Considerations for Requirements in §§ 1580.113, 1582.113, and 1584.11,* provides an analysis of the 9/11 Act's requirements and other considerations incorporated into the four categories of training required by this rule. *See* 81 FR at 91364.

[25] *See Request for Comments on Security Training Programs for Surface Mode Employees,* 78 FR 35945, 35948 (June 14, 2013) (discussion on grant-funded training programs under ''Relation to Other Training Programs''). TSA summarizes the response to the 2013 Notice in this final rule's RIA, Section 1.5. TSA explains in Sections 1.8.2. and 1.8.3. of the RIA how it used information from the responses to the 2013 Notice to assess the level of training in the baseline for PTPR and OTRB owner/operators, respectively.

[26] *See, e.g.,* Example of Security Training Matrix (TSA–2013–0005–0084) available in the docket to this rulemaking at *www.regulations.gov.*

[27] *See* sections III.G.5 and I of NPRM for a discussion of other related training. 81 FR at 91361–91362 and 91364 *et seq.*

implemented to comply with other Federal requirements or other standards in order to satisfy some or all of the requirements of this rule, the program submitted to TSA for approval must identify how the owner/operators intends to use the other training to satisfy TSA's requirements, such as the curriculum or lesson plan for that program. TSA intends to maintain an iterative list available to regulated owner/operators of training programs that have been approved by TSA for use in meeting this rule's requirements.

Paragraph (c)(2) requires an index to be provided if the owner/operator chooses to submit all or part of an existing security training program to TSA for approval. The index must be organized in the same sequence as the content requirements in §§ 1580.115, 1582.115, and 1584.115. Indexing is a necessary requirement if TSA is to provide flexibility for owner/operators to use existing training programs to satisfy this rule. TSA may request additional information on the program through the review and approval process.

J. What is the required schedule for providing training? (§ 1570.111)

1. Initial Training (§ 1570.111(a))

Current employees must be trained within one year of TSA's approval of the security training program. Initial training for new employees or those transitioning to a covered job function (as identified in Appendix B to parts 1580 (freight rail), 1582 (PTPR), and 1584 (OTRB)), must occur within the first 60 days of the date an employee begins to perform a security-sensitive function. In general, this means that an employee must be trained within 60 days of starting in a permanent-employment position that may require performance of a security-sensitive function, whether full or part-time.[28]

Section 1570.111(a)(3) addresses non-permanent employees. Non-permanent employees must receive training within 60 calendar days after employment that meets the definition of a security-sensitive employee. If an individual is employed on an intermittent or non-permanent basis, such as a contractor hired to perform a security-sensitive function for short durations, then the training must take place before the individual's aggregated length of employment by the owner/operator equals 60 calendar days within a consecutive twelve-month period. Training is *not* required if an individual is employed to perform a security-sensitive function one time for less than 60 days. Training *is* required if an individual performs a security-sensitive function for short but repeated durations and the aggregated period of time equals 60 days. TSA recognizes that some owner/operators may choose to train all regular contractors or other individuals employed for short but regular durations rather than having to monitor aggregated days of employment.

In meeting the initial training schedule, TSA expects that many owner/operators will rely on the provisions in § 1570.107, which provide standards for accepting previous training. TSA may allow ''training credit'' to be given for employees who received equivalent security training within one year before the rule's effective date. This training credit may include the following:

- Training on emergency preparedness plans that railroads connected with the operation of passenger trains must implement to address subjects such as communication, employee training and qualification, joint operations, tunnel safety, liaison with emergency responders, on-board emergency equipment, and passenger safety information.
- Training on policies that public transportation agencies implement to ensure safety promotion to support the execution of the Public Transportation Agency Safety Plan required under 49 CFR part 673 for all employees, agents, and contractors of any State, local government authority, or other operator of a public transportation system that receives Federal financial assistance under 49 U.S.C. Chapter 53.
- Training provided through funds granted under the Transit Security Grant Program or other grant programs.

The recordkeeping provisions, discussed below, require an owner/operator to provide current and former employees with documentation upon request of any training completed to meet the requirements of this rule. Options for compliance with this requirement could include providing employees with certificates to validate completed training. Providing employees with documentation of training is particularly relevant for operations such as those in the OTRB industry, where employees (for example, commercial drivers) may work for multiple owner/operators. If an owner/operator can validate an employee has received the required training within the specified timeframe, the training does not need to be repeated. Because of its obligation to ensure all training requirements are met, the current owner/operator is responsible for ensuring that any previous training courses satisfy the rule's requirements and documenting that the training was received within the required timeframe.

Finally, there may be situations where ''dual-hatted'' or other specific-function employees are required to receive security training from other sources as part of their jobs, such as railroad police officers employed by the owner/operator. As indicated above, it is the obligation of the owner/operator to ensure and document the training, including training received under these circumstances.

2. Recurrent Training (§ 1570.111(b))

TSA believes regular recurrent training is essential for transportation employees to maintain a high level of awareness and competency. To ensure this need is met, this rule requires owner/operators to provide the TSA-approved security training curriculum to their security-sensitive employees at least once every three years. This frequency is consistent with the requirements for security training imposed by the Pipeline and Hazardous Material Safety Administration (PHMSA) for hazardous materials employees under 49 CFR part 172.

In addition, consistent with 49 CFR 172.704, if the owner/operator modifies a security program or security plan for which training is required under this rule, the owner/operator must ensure that 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. This requirement ensures employees responsible for implementing the security program or plan will be trained in a timely manner concerning any changes or revisions to the security plan or program as necessary to reflect changes in security affecting their specific operating environment or the surface transportation system.

3. Previous Training (§ 1570.107)

While there is no specific requirement in the 9/11 Act for TSA to allow use of existing training programs to satisfy the security training regulatory requirements, this rule provides an opportunity for owner/operators to seek recognition of previously provided training. Under § 1570.107, an owner/operator may rely on previous training that occurred within the identified periods for initial or recurrent training.

[28] These deadlines are set by secs. 1408(d)(3), 1517(d)(3), 1534(d)3 of the 9/11 Act, codified at 6 U.S.C. 1137, 1167, and 1184.

In order to use previous training, the owner/operator must validate that the previous training satisfies the requirements of this rule (for example, reviewing records of training and curriculum), is relevant to the employee's job function, and appropriate for owner/operator's operations. As part of its inspection and compliance authority, TSA may require the owner/operator to provide the documentation used to determine the previous training met the requirements of this rule.

K. Do employees have to pass a test? ((§§ 1580.113(b)(9), 1582.113(b)(9), and 1584.113(b)(9))

TSA is not requiring security training programs to include employee testing, with prescribed pass/fail rates. The security training programs submitted to TSA, however, must include how the owner/operator will measure the effectiveness of the training program. TSA will afford flexibility to each individual owner/operator to identify measures for determining the effectiveness of their security training program using methods and criteria appropriate for their operations. For example, TSA expects that some owner/operators will choose to administer a written test or evaluation to gauge their employees' level of knowledge in order to assess the overall effectiveness of training, while others may rely upon operational tests conducted by supervisors to determine whether employees are being trained effectively. Some may use the results of drills and exercises to measure effectiveness and identify areas where modifications are needed.

Similarly, TSA is not prescribing conditions for a pass/fail policy that may be associated with post-training testing. While individual companies may elect to enforce pass/fail criteria with associated personnel actions, TSA is neither requiring nor recommending a specified maximum number of times that an individual may take a test or evaluation to demonstrate knowledge and competency. As previously noted, however, the methods submitted by an owner/operator for determining training efficacy may affect TSA's approval of any alternative measures for compliance. In reviewing security training programs, TSA's focus is on whether the program includes measures for the effectiveness of the training *program,* not an individual employee's performance.

III. Operational Requirements (Subpart D)

TSA requires freight and passenger railroad carriers, rail transit systems, rail hazardous materials shippers, and certain rail hazardous materials receivers, to appoint ''rail security coordinators'' [29] (RSCs) and report significant security concerns to TSA.[30] The RSCs are security liaisons to TSA, providing a single point of contact for receiving communications and inquiries from TSA concerning threat information or security procedures, and coordinating responses with appropriate law enforcement and emergency response agencies. This information, reported to TSA from the frontline of rail operations, is consolidated and analyzed by TSA to identify developing threats and trend analysis.

TSA is expanding applicability of these requirements to the owner/operators subject to the security training requirements. As a result, the scope of the requirement applies to:

- All rail operations subject to the security coordinator and reporting requirements under previous 1580.101, 1580.105, 1580.201, and 1580.203 (now located in sections 1570.201 and 1570.203);
- Any bus operations of a public transportation owner/operator required to provide security training under this rule; and
- Any OTRB owner/operator required to provide security training under this rule.[31]

As proposed in the NPRM, the rule text for applicability of the security coordinator requirements erroneously included all bus-only public transportation systems, TSA intended, however, to limit applicability to the bus-only public transportation systems within the scope of the security training requirements, that is, the higher-risk bus-only systems.[32] To be consistent with TSA's intent as explained above and in the preamble of the NPRM, TSA is clarifying the requirement in the final rule text.

Table 2 compares applicability scope of the previous requirement with the expanded applicability. The cost estimate for this requirement in the NPRM is consistent with TSA's intent and the corrected rule text.

TABLE 2—COMPARISON OF APPLICABILITY FOR SECURITY COORDINATOR AND REPORTING REQUIREMENTS

	Previous §§ 1580.101/103 and 1580.201/203	New §§ 1570.201/203
Freight railroad carriers	X	X
Rail hazardous materials shippers	X	X
Rail hazardous materials receivers in High Threat Urban Areas (HTUAs)	X	X
Owner/operators of private rail cars*	X	X
Railroads hosting freight or PTPR rail operations	X	X

[29] These requirements were promulgated in 2008, *see supra* n. 8, codified at 49 CFR 1580.101 and 1580.201 (before changes made by this rule).

[30] *See id.* at 49 CFR 1580.105 and 1580.203 (before changes made by this rule).

[31] As previously noted, TSA currently requires security coordinators for rail operations, including freight railroads, passenger railroads, and public transportation rail operations. In addition to mandating security coordinators for railroads, the 9/11 Act also requires security coordinators for bus operations. *See* 9/11 Act sec. 1531, codified at 6 U.S.C. 1181(e)(1)(A) (''Identification of a security coordinator having authority—(i) to implement security actions under the plan; (ii) to coordinate security improvements; (iii) to receive immediate communications from appropriate Federal officials regarding over-the-road bus security''). *See* 9/11 Act sec. 1512, codified at 6 U.S.C. 1162(e)(1)(A). For a similar provision applicable to railroads. Consistent with this mandate, TSA is extending the requirement to appoint a primary and at least one alternate security coordinator for OTRB companies and bus operations of PTPR owner/operators identified as higher-risk through this rulemaking. This will have a limited impact on the PTPR mode as most public transportation bus agencies covered by this rule are part of a larger system that is already required to have a security coordinator under current 49 CFR part 1580. *See* sec. III.D.4 of the NPRM for more discussion regarding the security coordinator and reporting requirements (81 FR at 91350 *et seq.*).

[32] *See* 81 FR at 91350: ''Because of the benefits of [the security coordinator and reporting requirements] to transportation security, TSA is proposing to extend these requirements to the modes of transportation covered by this proposed rule that are not currently subject to the requirements of 49 CFR part 1580. . . . TSA proposes to extend the requirement to appoint a primary and at least one alternate security coordinator for OTRB companies and the bus operations of PTPR owner/operators (with a limited impact as most public transportation bus agencies are part of a larger system that is required to have a security coordinator under current 49 CFR part 1580).''

TABLE 2—COMPARISON OF APPLICABILITY FOR SECURITY COORDINATOR AND REPORTING REQUIREMENTS—Continued

	Previous §§ 1580.101/103 and 1580.201/203	New §§ 1570.201/203
PTPR operating rail transit systems on general railroad system, intercity passenger train service, and commuter train services	X	X
PTPR operating rail transit systems not part of general railroad system	X	X
PTPR operating bus transit or commuter bus systems in designated areas		X
Tourist, scenic, historic, and excursion rail owner/operators*	X	X
OTRB owner/operators providing fixed-route service in designated areas		X

* Security Coordinator only required if notified by TSA in writing that a threat exists. Requirement to report significant security concerns always applies.

A. Security Coordinator Requirements (§ 1570.201)

Security coordinators are a vital part of transportation security, providing TSA and other government agencies with an identified point of contact with access to company leadership and knowledge of the owner/operators' operations, in the event it is necessary to convey extremely time-sensitive information about threats or security procedures to an owner/operator, particularly in situations requiring frequent information updates. The security coordinator and alternate provide TSA with a contact in a position to understand security problems; immediately raise issues with, or transmit information to, corporate or system leadership; and help recognize when emergency response action is appropriate. The individuals must be accessible to TSA 24 hours per day, 7 days per week.

The rule does not change the expectation that the security coordinator and alternate be appointed at the headquarters level. Nor does the rule require the security coordinator or alternate to be a dedicated position who has no other primary or additional duties. As with the previous part 1580 requirements, TSA's primary concern is having a designated point of contact available to TSA at all times.

The rule also requires the owner/operator to submit contact information for both the security coordinator and alternate and to update this information within 7 days if it changes. As previously noted, this is not a new requirement for owner/operators of railroads, including the rail transit operations of PTPR owner/operators. If an owner/operator subject to this rule has provided current information for primary and alternate RSCs to TSA, it will not have to take further action to meet the requirement.[33] TSA assumes this is true for passenger rail carriers, freight railroad carriers, and rail transit systems operated by public transportation agencies. Owner/operators required to appoint security coordinators for the first time under this rule must provide this information to TSA by July 29, 2020. TSA will also use this contact for communications related to requirements in this rule.

B. Requirement To Report Security Concerns (§ 1570.203)

As with the security coordinator requirement, TSA is moving and consolidating the requirement to report security concerns from part 1580 into § 1570.203 and extending it to higher-risk bus operations.[34] The list of reportable incidents can be found in Appendix A to part 1570 and includes not only a list of incidents, but descriptions and examples to assist regulated parties in making a determination of whether an incident must be reported based on its similarity to one of the examples.

This list of reportable significant security concerns is consistent with the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The NSI is a partnership between Federal, State, local, tribal, and territorial law enforcement that ''establishes a national capacity for gathering, documenting, processing, analyzing and sharing SAR information . . . in a manner that rigorously protects the privacy and civil liberties of Americans.'' [35] The NSI defines ''suspicious activity'' as ''observed behavior reasonably indicative of pre-operational planning associated with terrorism or other criminal activity.'' [36] The standardized approach among law enforcement officers and security officials with surface transportation entities produces more informative reports that can, more effectively, focus investigative efforts and intelligence analysis for potential trends and indicators of terrorism-related activity.

Finally, consistent with TSA's purpose in requiring submission of the information, the rule requires notification within 24-hours of the initial discovery of the incident by the owner/operator (*see* 49 CFR 1570.203(a)).[37] This schedule will enable TSA to obtain timely information, without undermining the ability of the owner/operator to appropriately handle a situation. If there is an immediate threat, owner/operators and/or their employees should prioritize notifying and working with first responders. The notification to TSA should occur after the immediate crisis is addressed, but within a timeframe that allows TSA to assess and share timely information.

For purposes of this requirement, the clock ''starts running'' when the owner/operator becomes aware of the incident. Awareness of the owner/operator includes awareness of (or discovery by) employees of the owner/operator.[38] TSA recognizes that local law enforcement do not always immediately notify owner/operators when there is a security-related incident on the owner/operator's property or affecting their operations.

C. Methods for Reporting Information and Substance of Information Provided (§ 1570.203 (a) and (c))

As previously noted, TSA has almost a decade of experience with incidents reported by railroads. Based on this experience, TSA recognizes that its ability to analyze the data and improve

[33] Any changes to the information must, as previously required, be reported within seven calendar days of the change taking effect.

[34] This extension is within TSA's discretion to require other actions or procedures determined to be appropriate to address the security of public transportation and OTRB operations. *See* 9/11 Act sections. 1405(c)(2)(I) and 1531(e)(1)(H), as codified at 6 U.S.C. 1134 and 1181, respectively.

[35] *See* Nationwide SAR Initiative (NSI), ''About the NSI'' (accessed Nov. 3, 2016), available at *http://nsi.ncirc.gov/about_nsi.aspx.*

[36] *Id.*

[37] This change to reporting is a modification from the requirement as promulgated in the Rail Security Rule, which required immediate reporting.

[38] One of the required training elements includes how to appropriately report security issues.

the quality of information disseminated back to its stakeholders is proportional to the quality of information it receives. Section 1570.203(b) is consistent with the reporting requirements as promulgated in 2008, which reflected the need for detailed and verified information from individual owner/operators to enhance TSA's ability to provide timely and useful information products to all of the relevant stakeholders.

TSA is working on two initiatives that should assist owner/operators with reporting information. The first is to pilot an electronic reporting option for significant security concerns.[39] If made a permanent capability, TSA intends to develop an online form that owner/operators, or their designated employees, may use to submit information to TSA to meet the requirements of this rule. If the pilot succeeds, TSA may pursue a second initiative to provide an electronic reporting form on a secure website. TSA will provide updates on development of these capabilities to owner/operators through the designated security coordinators as well as appropriate notices in the **Federal Register**. Pending completion of these capabilities owner/operators and their designated employees are generally required to meet the requirements of this section by contacting the Transportation Security Operations Center at 1–866–615–5150. There is an exception for owner/operators participating in the pilot to report electronically.

IV. Security Program Procedures

A. Deadlines Related to Submission and Approval of Security Training Program

Section 1570.109 identifies the required deadlines for submitting security training programs and the process for TSA approval. In general, not later than 90 days from the effective date of this final rule, owner/operators are required to submit programs to TSA in a form and manner prescribed by TSA. Owner/operators commencing new businesses or operations triggering applicability are required to submit their security training programs to TSA no less than 60 days before commencing operations.

TSA will provide details for submission of security programs directly to security coordinators identified under section 1570.201, within 10 business days from the effective date of this final rule. Consistent with comments received on the NPRM, this information will include the designated email address and any related information regarding submission of Sensitive Security Information (SSI).

As required by the 9/11 Act, TSA will review the programs within 60 days of receipt and either approve them or specify changes that are needed for approval.[40] If TSA requires changes, the owner/operator must submit a modified training program that meets TSA's specifications within 30 days of notification by TSA. TSA provides an analysis of burden and estimated costs associated with this information collection in section VIII.A. of this preamble and the Office of Management and Budget (OMB) 83–I Supporting Statement for its information collection request, which is available in the docket for this rulemaking.

B. Amendments

Procedures related to revision and/or amendment of security training programs, as described in §§ 1570.113, 1570.115, and 1570.117, are necessary as part of developing a regulatory program and are consistent with the 9/11 Act's requirements for implementation and submission of programs. These procedures are also consistent with TSA's statutory authority to allow exemptions from regulatory requirements.[41] The rule provides for two types of amendments: (1) Amendments initiated by owner/operators and (2) amendments initiated by TSA.

1. Amendments Initiated by Owner/Operator (§ 1570.113)

Under section 1570.113, there are three situations which require owner/operators to submit a request to amend their security training programs: (1) Changes affecting ownership or control of the operations; (2) changes to conditions affecting security; and (3) changes to content in the security training program. Owner/operators must seek an amendment if any of these changes are expected to have a duration of more than 60 days.

Amendments related to changes in ownership/control are necessary for TSA to maintain current information about relevant contacts as well as for purposes related to enforcement and liability. Amendments related to the second and third categories are necessary to ensure the training programs are providing relevant and timely information to security-sensitive employees.

This final rule revises the NPRM's proposed requirement for seeking an amendment for any changes relating to ''measures, training, or staffing described in the security program.'' Since publication of the NPRM, TSA determined that the scope of this requirement is too broad as it could capture measures relevant to security in general, such as theft. As proposed, the requirement could impose an unnecessary burden on owner/operators and create conflict between the programmatic requirements. For example, the overly broad requirement for amendments could result in the need to revise a security training program to address issues not related to reducing the risk of terrorism-related incidents.

To narrow the scope of the amendment requirement, the final rule incorporates a specific list of the types of changes to security that require an amendment. For purposes of identifying what types of changes should be included in the list, TSA determined the most appropriate source is the 9/11 Act's requirements for TSA to issue a vulnerability assessment and security planning regulation for surface owner/operators.[42] The 9/11 Act's provisions are tailored to security issues related to reducing the risk of terrorism-related incidents.

If an owner/operator makes any changes to the security measures identified in § 1570.113, the owner/operator must request an amendment to modify the TSA-approved security training program to align with these changes. In general, the program must be amended if there are changes to procedures intended to prevent and detect unauthorized access to restricted areas; measures to be implemented in response to periods of heightened security risk; and changes to emergency response plans.

The security program requirements established by this rulemaking will also be applicable to a future rulemaking to address the 9/11 Act's requirements for

[39] *See* OMB Control No. 1652–0051, 30-Day Notice: *Revision of Agency Information Collection Activity Under OMB Review: Rail Transportation Security,* 83 FR 40542 (Aug. 15, 2018), and related supporting statement available at *https://www.reginfo.gov/public/do/PRAViewDocument?ref_nbr=201809-1652-002.*

[40] *See* 9/11 Act secs. 1137(d)(2), 1167(d)(2), and 1184(d)(2), codified at 6 U.S.C. 1137, 1167, and 1184.

[41] *See* 49 U.S.C. 114(q).

[42] As previously discussed, the 9/11 Act includes a mandate for TSA to issue regulations requiring vulnerability assessments and security plans in addition to the requirements for security training. *See* 9/11 Act sections 1405, 1612, and 1531, codified at 6 U.S.C. 1134, 1162, and 1181, respectively. The security planning requirements include a detailed list of security measures that must be incorporated into an owner/operator's TSA-approved security plan. TSA intends to address the vulnerability assessment and security training requirements through a separate rulemaking.

vulnerability assessments and security planning. As a result, incorporating the 9/11 Act's list of security measures to be incorporated in security planning as the basis for determining when an amendment is necessary to a security training program establishes a framework that can be consistently applied in the future as the scope of requirements for higher-risk owner/operators of surface transportation systems is expanded.[43]

Finally, owner/operators must request an amendment if their security training program is modified, including modifications related to addressing the effectiveness of the program or development of recurrent training materials that differ from the initial training. This provision is intended to ensure an owner/operator is appropriately addressing the results of its TSA-approved method for determining effectiveness of security training.[44] It is TSA's intent that this specificity will reduce the burden for owner/operators by providing clarity on the types of changes that may trigger the need for an amendment. If there are any changes in these areas, it is reasonable to expect that some aspects of the security training program must be revised.

In addition to the preceding issues that require owner/operators to request an amendment, the same procedures can be used when the owner/operator seeks to amend its program to address other operation issues. For example, an owner/operator may choose to seek an amendment to modify the required training schedule. The same procedural requirements for seeking an amendment apply.

TSA may approve an amendment if it is in the interest of public and transportation security and meets the required security standards. As part of its standard practice for security program administration, TSA works with owner/operators on amendment requests to develop options acceptable to both TSA and the requesting owner/operator. TSA may ask for additional information from the owner/operator or require more time in order to makes its determination.

If TSA is unable to come to agreement with the owner/operator on the content or scope of the amendment, TSA may deny the amendment request. The denial will include a statement of why the request is denied. The owner/operator can petition for reconsideration under section 1570.119.

While the rule only requires amendments if the change is to be permanent (defined as 60 or more calendar days), TSA recognizes that there are times when a change of short duration could have a significant impact on training. For example, if a city is hosting a National Special Security Event (NSSE), the public transportation system serving that city may implement additional security measures. It is likely that additional training will be necessary to raise appropriate awareness of these additional measures. The rule does not require the owner/operator to request an amendment to provide this additional training.

TSA is also modifying the schedule for submitting an amendment from the requirement as proposed in the NPRM. Under the NPRM, an amendment had to be submitted no later than 45 days before the change takes effect. This schedule does not work with the provision that allows changes to security measures to be in effect for 60 days before they are considered permanent, and only permanent changes require notification and amendment. To address this inconsistency, TSA is requiring amendments to be submitted within 65 days of the change. As the owner/operator controls changes to the security measures identified in the rule and whether these changes will be permanent, it is presumed the owner/operator will have sufficient advance notice that an amendment is needed and can prepare and submit the request within this timeframe. This specificity is added to provide clarity for compliance.

2. Amendments Initiated by TSA (§ 1570.115)

TSA may require amendments in the interest of the public and transportation security. As indicated in § 1570.115, TSA may require owner/operators to revise their training based on emerging threats or methods for addressing emerging threats. This is consistent with TSA's authorities under 49 U.S.C. 114 and the 9/11 Act, which specifically provide that TSA must update the requirements, as appropriate, ''to reflect new or changing security threats.'' [45] For example, the curriculum requirements identified in the 9/11 Act do not address training to respond to active shooter incidents. Following several active shooter incidents, including one that resulted in the death of a Transportation Security Officer in Los Angeles, Congress prioritized the need for this type of training.[46] TSA could also require an amendment to provide additional training to address risks like the NSSE discussed above, in section C. As with other requirements imposed by TSA, the owner/operator may request a petition for reconsideration of TSA-required amendments.

C. Alternative Measures (§ 1570.117)

Section 1570.117 includes the procedures for requesting a waiver, procedures for requesting the use of alternative measures, and identification of the types of information TSA will need in order to make a decision to grant such requests. TSA may grant such a request under the authority 49 U.S.C. 114(q), based on a determination that the alternative measure or exemption is in the public interest. In general, TSA will consider factors such as risk associated with the type of operation, current threat information, and any other factors relevant to potential risk to the public and transportation security if the request is granted.

These procedures can be used by an owner/operator to request alternative measures to satisfy all of some or all of the requirements of subchapter D. For example, the owner/operator could request to extend the time period for submitting its training program or for training all of its security-sensitive employees. An owner/operator could also request a waiver from some or all of the regulatory requirements. For example, a freight railroad may meet the criteria for applicability, but the operations that trigger applicability may be a *de minimis* part of its overall business operations. In such a situation, the owner/operator might consider requesting either a complete waiver or an alternative that limits the requirements to a more discrete part of its business.

D. Petitions for Reconsideration (§ 1570.119)

Section 1570.119 describes the review and petition process for TSA's reconsideration when it denies a request for amendment, waiver, or alternative measures, as well as a TSA requirement

[43] *See* discussion *supra* in n. 42

[44] *See* requirements in subpart B to parts 1580, 1582, and 1584.

[45] *See* 9/11 Act at 1408(d)(4), 1517(d)(4), and 1534(d)(4), codified at 6 U.S.C. 1137, 1167, and 1184, respectively. This provision also requires owner/operators change their programs to address TSA's requires updates and retrain employees as necessary, within a reasonable time.

[46] Section 7 of the *Gerardo Hernandez Airport Security Act of 2015* (Pub. L. 114–50), which directed TSA, in consultation with the Department of Transportation and other relevant agencies, to conduct outreach to all passenger transportation agencies and providers of high-risk facilities to verify such agencies and providers have in place plans to respond to active shooters, acts of terrorism, or other security-related incidents that target passengers.

to modify or amend a program. If an owner/operator seeks to challenge the decision, the owner/operator is required to submit a written petition for reconsideration within the time frame identified in the applicable section. The petition must include a statement, with supporting documentation, explaining why the owner/operator believes the reason for the denial or for the amendment, as applicable, is incorrect. If the owner/operator requested the amendment, the results of the reconsideration could be confirmation of TSA's previous denial or approval of the proposed amendment. If the issue involves a TSA-required amendment, the results of the reconsideration could be withdrawal, affirmation, or modification of the amendment. A disposition pursuant to 49 CFR 1570.119 occurs when the Administrator or designee has disposed of the petition by affirming, modifying, or rescinding the previous decision. Such disposition constitutes a final agency action for purposes of review under 49 U.S.C. 46110.

E. Recordkeeping Requirements (§ 1570.121)

The final rule requires owner/operators to create and maintain lists of their security-sensitive employees and specify when these employees received the required training. Training records must include each trained employee's name, job title or function, date of hiring, and date and course information on the most recent security training that each employee received. Records for individual employees must reflect the training courses completed and date of completion. Records of an employee's initial and recurrent training must be maintained by owner/operators for no less than five years from the date of the training and available at the location(s) specified in the security training program approved by TSA.

The final rule provides flexibility to owner/operators to decide whether to maintain the records in electronic format provided that (1) any electronic records system used is designed to prevent tampering, loss of data, or corruption of records, and (2) paper copies of records, and any amendments to these records, must be made available to TSA upon request for inspection or copying. Whether the records are kept in electronic or other form, the employee must be provided with proof of training upon request, at any time during the three-year recordkeeping period, without regard to the requestor's current status as an employee of that entity. As discussed above in II.J. (Initial Training), owner/operators may meet the proof-of-training requirement by providing a certificate, letter, or other similar documentation to the employee upon completion of training. In order for TSA to allow any owner/operator to rely upon previous security training to satisfy the requirements of this rule, it is critical that employees be able to validate whether they received previous training.

TSA assumes training records are unlikely to include SSI, but nonetheless provides a reminder in this provision that any SSI maintained as a result of these recordkeeping requirements must be maintained consistent with the requirements in 49 CFR part 1520. For example, an owner/operator may decide to keep a copy of the content of the training program with the employee files (which is not required by the rule). If the curriculum contains SSI information, any file it is in must be stored as required by the SSI regulations. Owner/operators needing additional information about appropriately maintaining SSI may contact TSA for assistance and/or find information on TSA's website.[47]

F. Summary of Deadlines

The following table summarizes the deadlines for the preceding programmatic requirements. The information is provided for operations that exist on the effective date of this rule and those that may commence or trigger applicability based on future modifications.

TABLE 3—SUMMARY OF DEADLINES FOR COMPLIANCE

Requirement	Dates		
	Existing operations	New or modified operations	New employees (hired after TSA approves the security program)
Effective date of rule	June 22, 2020.		
Deadline for notifying TSA of applicability determination (1570.105).	July 22, 2020	90 calendar days before commencing new or modified operations.	
Deadline for providing security coordinator information to TSA (1570.201).	July 29, 2020	7 calendar days after commencement of operations.	
Deadline for submission of security training program to TSA for approval (1570.109(b)).	90 calendar days from effective date.	90 calendar days after commencing new or modified operations.	
TSA approval or notification of required modification (1570.109(c)).	60 calendar days from receipt of security training program.	60 calendar days from receipt of security training program.	
Initial training of security-sensitive employees (1570.111(a)).	1 year from TSA approval of security training program.	1 year from TSA approval of security training program.	60 calendar days after employee first performs a security-sensitive job function (60th day, aggregated over 12-month period, if intermittent employee).
Recurrent training of security-sensitive employees (1570.111(b)).	Within three-years of the date of initial training and every three-years thereafter.	Within 90 days of changes to security program or security plan affecting employees' security-related responsibilities.	

[47] *See https://www.tsa.gov/for-industry/sensitive-security-information.*

V. Miscellaneous Changes

This final rule includes the following changes to other provisions in TSA's regulations as necessary to implement these requirements.

A. Amendments to Part 1500

Consistent with the rule's organization, TSA includes definitions for terms relevant to several subchapters of TSA regulations, beyond the requirements of subchapter D, in part 1500. Terms only relevant to the provisions in subchapter D are incorporated in § 1570.3. Terms uniquely relevant to each mode or the other requirements in subchapter D are incorporated into the relevant parts.

As noted in the NPRM, TSA is meeting a 9/11 mandate to define, through notice and comment rulemaking, the term ''security-sensitive material.'' To meet the requirement, TSA is incorporating by reference the definition of hazardous materials for which a security program is required under 49 CFR 172.800(b), promulgated by PHMSA through notice and comment rulemaking and in consultation with TSA.[48] There are no current TSA-programmatic requirements linked to this definition. A full discussion of amendments to the terms in part 1500 is provided in the NPRM.[49]

B. Amendments to Part 1503

TSA is making minor amendments to part 1503 (Investigative and Enforcement Procedures), as necessary, to conform these regulations to changes made by this final rule. In § 1503.101(b), the scope of statutory provisions is amended to add authorities from the 9/11 Act that are administered by the TSA Administrator. These are conforming amendments with no cost impact.

C. Amendments to Part 1520

TSA is also finalizing proposed modifications to part 1520 (Protection of Sensitive Security Information). As discussed in the NPRM, these changes are necessary to conform the SSI provisions to include the transportation security-related requirements in this rule.[50] The amendments are limited to: (1) Eliminating unnecessary terms from part 1520 that are added to part 1500 and (2) replacing the limiting term ''rail transportation security requirement'' with ''surface transportation security requirement.'' In some places, such as the definition of ''vulnerability assessment'' in § 1520.3, TSA is streamlining a lengthy description of types of transportation to simply state ''aviation, maritime, or surface transportation.''

The impact of these revisions should also be minimal. Under § 1520.7(j), any person who has access to SSI is required to protect it according to the requirements of the regulation. Most of the population affected by this rule has previously received SSI information from TSA, as well as training on the proper handling of SSI, and have procedures in place to ensure the requirements of the regulation are met.[51]

D. Amendments to Part 1570

Because of the significant restructuring of part 1570, as discussed above, the rule text includes the entire part. In addition, TSA is adding a provision related to security responsibilities and relocating to this part the provisions related to compliance, inspection, and enforcement (previously in part 1580).

1. Security Responsibilities for Employees and Other Persons (§ 1570.7)

Under § 1570.7, the obligation for compliance is not limited to owner/operators specifically referenced under applicability provisions. Rather, any person may be held to have violated these rules, including contractors who provide service to owner/operators and the employees of such contractors. This provision in subchapter D ensures a uniform application of TSA's enforcement policy across all modes of transportation, consistent with TSA's authority under 49 U.S.C. 114(f).[52] In addition to violations for failure to comply with requirements, TSA can also pursue enforcement actions for interfering with compliance or hiding evidence of non-compliance. Contractors are also subject to inspection for compliance with this rule and enforcement actions, as discussed below.

2. Compliance, Inspection, and Enforcement (§ 1570.9)

TSA is mandated to: (1) Enforce its regulations and requirements; (2) oversee the implementation and ensure the adequacy of security measures; and (3) inspect, maintain, and test security facilities, equipment, and systems for all modes of transportation.[53] This mandate applies even in the absence of rulemaking, but TSA has chosen to include a restatement of its authority in its rules. The statute specifically requires TSA to—

- Assess threats to transportation;
- Enforce security-related regulations and requirements;
- Inspect, maintain, and test security of facilities, equipment, and systems;
- Ensure the adequacy of security measures for the transportation of cargo;
- Oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;
- Require background checks for airport security screening personnel, individuals with access to secure areas of airports, and other transportation security personnel; and
- Carry out such other duties, and exercise such other powers, relating to transportation security as the Administrator considers appropriate, to the extent authorized by law.

While current part 1570 includes a provision stating TSA's compliance, inspection, and enforcement authority, it is not provide the same detail found in other regulatory provisions.[54] Therefore, TSA is transferring the text of current § 1580.5 to subpart A as § 1570.9, with minor modifications to reflect the addition of certain bus operations that have previously been unregulated by TSA.[55]

3. ''Covered Person'' (§ 1570.305)

This final rule includes a technical correction to § 1570.305 (currently § 1570.13) of subchapter D as part of this rulemaking. This provision prohibits public transportation agencies and rail carriers from knowingly misrepresenting Federal guidance or regulations related to security background checks for certain individuals.[56] The definitions in the section currently include the term ''covered individual,'' which may result in confusion as to whether the term has the same meaning as ''covered person'' in TSA's programs to address access to SSI.[57] To eliminate any potential for confusion, this rule amends § 1570.305

[48] *See* 81 FR at 91344.

[49] *See* section III.A. of the NPRM. 81 FR at 91342 *et seq.*

[50] *See id.* at 91343–91345.

[51] *See https://www.tsa.gov/for-industry/sensitive-security-information.*

[52] *See* 49 U.S.C. 114(f)(7) and (11). A similar provision applicable to aviation employees and other related persons is in 49 CFR 1540.105(a)(1) and (b).

[53] *See* 49 U.S.C. 114(f).

[54] Compare current § 1570.11 with current § 1580.5. The provision in part 1580 is also consistent with 49 CFR 1542.5, 1544.3. 1546.3, 1548.3, and 1549.3.

[55] A more detailed discussion of current § 1580.5, still relevant to the section, can be found in the preamble for current part 1580. *See* 71 FR 76852 (Dec. 21, 2006) and the Rail Security Rule, *see supra* n. 8. (Final Rule).

[56] This final rule moves this section from § 1570.13 of subchapter D to section § 1570.305. The requirement was added to address another 9/11 Act requirement. *See* 73 FR 44665 (July 31, 2008) for more information on the rulemaking that added this provision.

[57] *See* 49 CFR 1520.7.

to delete the definition and consistently use the term ''employee'' (as defined by this rulemaking in § 1570.3) rather than ''covered individual.'' This change is for clarification purposes only and has no substantive impact.

VI. Summary of Changes

The following table summarizes changes between the NPRM and final rule.

TABLE 4—SUMMARY OF CHANGES BETWEEN NPRM AND FINAL RULE

Section No.	Section title	Change from NPRM	Implication
1570.111(b)	Implementation schedules (recurrent security training).	In response to comments, TSA is modifying the recurrent security training schedule to a three-year cycle rather than annual. Changes to security programs and plans may require training certain employees within 90 days of the changes.	Cost Savings.
1570.113	Amendments requested by owner/operator.	NPRM proposed requiring owner/operators to request an amendment to their security training programs when there are changes to (a) ownership or control of operations and/or (b) measures, training, or staffing described in the security program. The final rule includes a specific list of the types of changes that would trigger the need to update the security training program. The NPRM also proposed to require an amendment to be filed within 45 days before the amendment takes effect. The final rule requires an amendment to be requested no later than 65 days after the change to the security program/measures/plans takes effect.	TSA recognizes that some owner/operators may have security programs that address issues not related to transportation security, such as theft or vandalism. TSA is narrowing the scope of the requirement to reduce the burden. The final rule identifies the types of issues that would require amendment. The list of issues used by TSA is consistent with the requirements for security plans in sections 1405, 1512, and 1531 of the 9/11 Act. Modifying the deadline for requesting an amendment is intended to provide clarity for compliance and be more appropriate for the types of amendment-requests TSA expects to receive.
1570.201	Security coordinator	NPRM proposed requiring all public transportation agencies to have a security coordinator. Final rule limits the scope of the requirement to rail operations of public transportation agencies and the bus-only operations of those determined by TSA to be higher-risk.	The scope of this requirement in the NPRM was broader than TSA intended as the result a drafting error. TSA intended the security coordinator requirement to apply to all of the rail operations and shippers/receivers covered by the Rail Security Rule, plus bus operations required to provide security training under this rule.
1570.203	Reporting significant security concerns.	NPRM proposed requiring all public transportation agencies to report security issues. Final rule limits the scope of the requirement to rail operations of public transportation agencies and the bus-only operations of those determined by TSA to be higher-risk.	The scope of this requirement in the NPRM was broader than TSA intended as the result of a drafting error. TSA intended the reporting requirement to apply to all of the rail operations and shippers/receivers covered by the Rail Security Rule, plus bus operations that are required to provide security training under this rule.
1570.305	False statements regarding security background checks by public transportation agency or railroad carrier.	TSA is making a technical correction to this provision by replacing the term ''covered individual,'' with the term ''employee,'' which is defined by this rulemaking in § 1570.3.	This technical revision eliminates potential confusion in the terminology.

VII. Response to Comments on NPRM

Following TSA's publication of the NRPM on December 16, 2016, industry associations, unions, and private citizens were among those who submitted comments in docket TSA 2015–0001. TSA's responses are organized by topic.

A. General Comments

1. Need for Rule

Comments endorsing the rulemaking and recommending an expanded scope: A number of submissions included a statement of general support for TSA to issue this rulemaking. Commenters also endorsed the rule, noting that proper training could prevent harm to both employees and passengers. A few commenters suggested expanding the scope of the rulemaking to include additional training for surface workers, such as self-defense training, or to provide training to all American citizens to identify terrorist threats. One commenter supported a ''community of the whole'' approach, reflecting the collaborative and cooperative partnership between TSA and industry to detect and deter individuals seeking to commit acts of terrorism.

TSA response: This rulemaking is intended to solidify a baseline of security training. Promulgation of this rule does not signal a change in TSA's commitment to maximize enhancements to surface transportation security through voluntary cooperation and collaboration. Consistent with this commitment, TSA does not believe it is necessary to expand the scope of applicability or requirements, but encourages owner/operators to provide additional security training as they consider appropriate to address potential vulnerabilities or threats within their unique operational environments. As noted in the NPRM, TSA encourages owner/operators covered by this rule to determine

whether there are employees not covered by the scope of the security-sensitive definition who could provide benefits to security if trained.

Regarding the recommended expansion of the rule to cover broader populations, including the general public, DHS has numerous programs and initiatives to provide and encourage awareness of terrorist threats and appropriate responses. These initiatives include ''hometown security'' and the ''See Something, Say Something'' campaign. More information on these initiatives and training available to support them can be found on the DHS website.[58] TSA also encourages owners/operators not within the scope of the rule's applicability to voluntarily provide security training to their employees, using the curriculum requirements in this rule to guide development of voluntary security training programs. As noted in section II.A., TSA also intends to provide resources developed to support this rule to other owner/operators, as appropriate.

Comments opposing rulemaking: Other commenters opposed the rulemaking, primarily because they believe certain modes already conduct training, and asserted these efforts make the rulemaking unnecessary. Three commenters expressed concern the rule overlaps with existing State and Federal training requirements, including the FRA's 2014 final rule, which established minimum training standards for all safety-related railroad employees.[59] One commenter suggested States may have different requirements, which should be considered in this rulemaking. Several commenters advocated for the rule to be voluntary, and noted voluntary training has so far produced exceptional results.

TSA response: As previously discussed, TSA has a statutory mandate to publish a final rule requiring security training for frontline employees of public transportation agencies, railroads, and OTRB owner/operators.[60] The statutory mandate includes specific requirements for the content of the required security training. In addition, TSA determined it is necessary to require security training for employees of higher-risk surface transportation operations and appropriate to use its general authority under ATSA to issue a rule including these requirements.[61]

The terrorism-related threat to surface transportation modes has not subsided and Congress has not retreated from its commitment to the need for this rule. Since enactment of the 9/11 Act, Members of Congress and the DHS Office of the Inspector General (OIG) have expressed continued interest in the publication of this rule.

This rulemaking is intended to solidify the baseline for security training of surface employees. TSA recognizes the substantial efforts of our stakeholders to enhance their security posture since 9/11 and seeks to recognize and build upon these efforts. As noted in the NPRM, owner/operators subject to requirements to provide similar training may request to use this training to satisfy requirements in this rule. For example, TSA is aware that many public transportation agencies and railroads currently provide security training to comply with State or Federal training requirements. (TSA is not aware of any overlapping requirements for OTRB owner/operators.) If an owner/operator intends to use previous training or existing training programs in order to satisfy some or all of the requirements of this rule, the program submitted to TSA for approval must identify how the other training satisfies TSA's requirements. This will likely necessitate submitting the curriculum or lesson plan for that program and training records, as well as information on the employees who have completed the training and the date of the most recent training.

Regarding voluntary training, TSA acknowledges many owner/operators of higher-risk surface transportation operations have voluntarily implemented security training programs addressing some of the requirements in this rule. As noted in the *Preliminary Regulatory Impact Analysis and Initial Regulatory Flexibility Analysis* (NPRM RIA), however, the private market may not provide adequate incentives for owner/operators to make an optimal investment in the full range of measures to reduce the probability of a successful terrorist attack based on the economics of externalities. Mandating security training for higher-risk operations will solidify the current baseline of security training established through voluntary measures.[62]

2. Cost of Rule

Comments: Some commenters expressed concern that the cost of the rulemaking is too high, and that the rule is too costly for industry to implement. Commenters also asserted the estimate of OTRB owner/operators is too low, and questioned whether TSA's cost-estimate analysis considers the Unfunded Mandate Reform Act of 1995 (UMRA).[63] One commenter generally suggested that the expense of providing security awareness training to surface transportation personnel may not be justified by the potential benefits. Another commenter, a mass transit agency in a large metropolitan area, estimated the cost of the rule to be higher than the estimate TSA provided in the NPRM RIA.

TSA response: A full discussion of the cost-benefit analysis is included in the *Final Regulatory Impact Analysis and Regulatory Flexibility Analysis* (Final RIA) [64] and summarized in section VIII.B.1. While training and the other requirements of this final rule are not absolute deterrents for a terrorist intent on carrying out attacks on surface modes of transportation, TSA expects the probability of success for such attacks to decrease when the requirements of this rule are fully implemented.

Regarding the commenters concerns that TSA's estimate of OTRB owner/operators within the scope of applicability is too low, TSA acknowledges the inherent uncertainty in this estimate due to the fluid and opaque nature of the industry. As described in the Final RIA, ''many [OTRB] owner/operators that operate charter and/or tour services also provide scheduled or fixed-route services, sometimes on an ad hoc basis, making it difficult for any one source to keep track of those that may provide scheduled service as part of their non-primary operation.'' [65] In response to the issue of disparate data, TSA consulted multiple sources and databases to build its estimate.' The commenter who stated the OTRB estimate was too low did not provide any reason to support the claim that TSA underestimated the number of affected owner/operators or any source/

[58] *See www.dhs.gov/hometown-security* and *www.dhs.gov/see-something-say-something.*

[59] *See* 79 FR 66460 (Nov. 7, 2014), codified at 49 CFR part 243.

[60] *See* discussion in section I.A. of this rule. *See also* 81 FR 91341 (discussion of statutory authorities and requirements for this rulemaking).

[61] *See* 81 FR 91339–91341 (discussion of purpose and authorities).

[62] *See* NPRM RIA at 116–117 (available in the docket to this rulemaking at *www.regulations.gov*).

[63] Public Law 104–4, 109 Stat. 48 (Mar. 22, 1995), codified at 2 U.S.C. 1501–1538.

[64] The Final RIA is available in the docket for this rulemaking at *www.regulations.gov.*

[65] *Id.* at 40. Note: Under the requirements of this rule, any owner/operators conducting ad hoc or sub-contracted service for a regulated person must comply with the requirements of the rule as an authorized representative. Similarly, an owner/operator not subject to the requirements of the rule may trigger applicability if they contract for ad hoc or subcontracted service through an area that triggers applicability.

data to back up the assertion. As mentioned in the NPRM RIA, TSA sought public contribution to refine its estimate, but neither the commenter nor anyone else provided any data or new information on which to build a different estimate.

Title II of UMRA, establishes requirements for Federal Agencies to assess the effects of their regulatory actions on State, local, and tribal governments and the private sector.[66] Agencies must prepare a written statement, including a cost-benefit analysis, for proposed and final rules with ''Federal mandates'' that may result in expenditures by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million or more in any one year.[67] TSA's analysis for both the NPRM RIA and Final RIA determined this rule does not contain a Federal mandate that may result in expenditures of $100 million or more either for State, local, and tribal governments in the aggregate, or for the private sector in any one year.

The commenter who stated security awareness training may not be justified by the potential benefits did not provide data to support this assertion. Based upon the data available to TSA, as shown in the Final RIA, TSA disagrees with the commenter. In both the NPRM and Final RIA, TSA includes a chapter, titled ''Benefits of Employee Security Training,'' which identifies the security risks to surface transportation and explained how providing employees with the knowledge to prepare, observe, assess, and respond to a terrorist related threat or incident reduces the vulnerability to a terrorist attack. In addition, TSA conducted a break even analysis that compared the cost of the surface training program to the direct economic losses that would be averted by avoiding certain terrorist attack scenarios. Given the relative small costs of implementing training compared to the catastrophic costs of a successful terrorist attack, this analysis found that the rule would only have to deter, at minimum, one attack every 40 years for the benefits to equal costs for freight rail, a number that increases to one attack every 166 years for OTRBs.[68] The monetized benefits of preventing an attack would likely be greater were TSA to conduct a break even analysis that accounts for the difficult-to-estimate macroeconomic and other indirect impacts (avoided indirect costs) that may be even more significant than the direct impacts of the attack. Avoided consequences, such as the value of a reduction in fear felt by the public at large, are not included in the analysis because they are difficult to measure and quantify. Given these results and the demonstrated effectiveness of employee training—including security awareness in mitigating terrorist attacks[69]—TSA believes the benefits of the rule justify its costs. Finally, as previously discussed, TSA is under a statutory mandate to publish a final rule requiring security training for frontline employees of public transportation agencies, railroads, and OTRB owner/operators.

One commenter, from a large metropolitan area public transportation system, provided information to support statements that the costs of implementing the rule would be higher than TSA estimated in the NPRM RIA for that commenter. TSA believes there are a number of issues with the commenter's estimate that result in an overestimation of the rule's burden. The commenter assumed the duration of training to be three hours when TSA estimates that training for security-sensitive employees of a PTPR owner/operator will likely average 1 hour and 20 minutes in order to address all of the required elements in this rule.[70] The commenter appears to base their three hour estimate on an assumption that a classroom setting and development of original course material is necessary. As further discussed below in section VII.D., TSA is not requiring instructor or classroom training and will further mitigate costs by providing a video, free of charge, to regulated owner/operators for compliance with the parts of the rule. TSA intends for this material to cover three of the four PTPR training elements in the rule and take less than one hour.

Finally, the commenter comes from one of the largest metropolitan areas in the United States with one of highest costs of living. This leads TSA to believe that the estimate provided by the commenter is likely higher than the national average of transit agencies. TSA used national wage data for transit agencies from the Bureau of Labor Statistics to estimate cost of the rule to PTPR owner/operators. TSA believes this is a reasonable rate to calculate incurred costs to regulated PTPR owner/operators because it encompasses the entire transit industry (which are typically found in cities around the country). Based on this analysis, TSA believes its cost-assessment for the final rule is representative of the incremental burden PTPR owner/operators will incur from implementing the regulatory requirements at a national level. However, TSA does acknowledge that differences in the cost of labor among the various cities may contribute to certain transit agencies having higher or lower costs than the national average.

3. Stakeholder Consultation

Comments: Several commenters suggested TSA consult with labor unions in drafting the rulemaking, as required by the 9/11 Act, and also reach out to international security experts.

TSA response: The 9/11 Act directed TSA to consult with major stakeholders during the development of the NPRM, including labor organizations. As noted and summarized in the NPRM, TSA conducted numerous meetings and conference calls with all necessary parties, including relevant labor organizations.[71] In addition to inviting participation of labor union representatives in many of the mode-specific meetings, TSA also met directly with labor unions as part of its stakeholder consultation process, including the Transportation Trades Department of the American Federation of Labor and Congress of Industrial Organizations, the International Brotherhood of Teamsters, the Brotherhood of Locomotive Engineers, and the Amalgamated Transit Union.[72]

International outreach is also a key component of TSA's transportation security mission. TSA surface representatives partner with the international community through a number of forums, such as INTERPOL, European Network of Railway Police Forces (RAILPOL), and the United Nations led International Working Group Land Transport Security (IWGLTS). These meetings include a regular exchange of lessons learned in addressing emerging threats within the surface transportation environment.

4. Terms

Comments on definition of ''transportation security-sensitive materials (TSSM)'': Several commenters

[66] *See supra* n. 63.

[67] *Id.* at sec. 202, codified at 2 U.S.C. 1532. The $100 million in 1995 dollars is adjusted for inflation to 2017 dollars using the GDP implicit price deflator for the U.S. economy. Bureau of Economic Analysis, *National Data,* Table 1.1.4. Price Indexes for Gross Domestic Product, Line 1 Gross domestic product. Available at: *https://apps.bea.gov/iTable/iTable.cfm?reqid=19&step=2#reqid=19&step=2&isuri=1&1921=survey.*

[68] *See* Final RIA at Section 4.3.

[69] *See id.* at Section 4.1 (full summary of the threat to surface transportation and an example of security training effectiveness).

[70] *See* Final RIA at Section 2.4 for an explanation and rationale to why TSA estimates 1 and 20 minutes needed to train mass transit agencies' security-sensitive employees on the training components of the final rule.

[71] *See* 81 FR 91336 at 91368–91370.

[72] *See id.* at 91370.

asked for clarification regarding how the TSSM definition applies to motor coaches, and suggested industry aid TSA in determining what should qualify as TSSM. One commenter asked TSA to provide handling and storage information regarding TSSM specific to the motor coach industry.

TSA response: As noted in the NPRM, TSA is satisfying a 9/11 Act requirement to define TSSM [73] by incorporating by reference the hazardous materials identified in 49 CFR 172.800(b). There are no specific requirements in the rule related to the definition. To the extent there are requirements associated with the materials identified in 49 CFR 172.800(b), persons should consult 49 CFR part 172, the hazardous materials rules promulgated by PHMSA. The PHMSA rules include security requirements related to these specific materials. The PHMSA requirements were promulgated through notice and comment rulemaking, including participation by relevant stakeholders in developing the list of materials.

Comments on definition of ''host railroad'': One commenter asserted the definition of ''host railroad'' is confusing. Additionally, the commenter noted TSA's expectations of the railroads responsible for ensuring training of employees in ''host'' situations are unclear, as railroads currently train employees under existing training programs.

TSA response: As noted in the NPRM,[74] TSA is defining ''host railroad'' consistent with the definition well-established by use for the rail industry under rules of the FRA.[75] Under this rule, both the host and tenant railroads are required to have a training program that appropriately addresses the ramifications of the hosting relationship. For example, the host railroad's training program will need to address the operational considerations of the hosting relationship, such as training dispatchers on their role and responsibilities in halting the tenant railroad's operations over a segment of track where there is a potential threat (such as a suspected IED or tampering with infrastructure). Similarly, a tenant railroad subject to the security training requirements of 49 CFR part 1582 (PTPR), will need to address the operational considerations of the hosting relationship, such as instructing its train and engine employees on the proper communication procedures to follow when a potential threat is identified. Under either example, the host and tenant railroad owner/operators will only be responsible for training their own employees.

When inspecting for compliance by regulated parties participating in a contractual relationship, TSA will consider the freight railroad carrier (the private company) to be an authorized representative of the PTPR owner/operator (the owner/operator of the passenger train service). TSA will hold the PTPR owner/operator primarily responsible for compliance and for ensuring that all security-sensitive employees receive the required training, whether they are employed directly by the PTPR owner/operator or contractor. The PTPR owner/operator must train the freight railroad carrier's employees performing security-sensitive functions related to the passenger train service.[76]

B. Investigative and Enforcement Procedures

Comments on penalties and violations under 49 CFR part 1503: Several commenters requested clarification regarding the exact penalties for non-compliance, and others asked TSA to explain the basis of violations.

TSA response: The 9/11 Act included authority for TSA to assess civil penalties for violations of title 49 of the U.S. Code, including surface transportation requirements.[77] TSA posts, and regularly updates, its sanction policies on its website.[78] Between this rule's date of publication and effective date, TSA will update this policy to address violations of this rule.

Comments on compliance, inspection, and enforcement under 49 CFR 1570.9: Several commenters expressed concern regarding how TSA will enforce the rule. One commenter suggested TSA and relevant DOT components should develop a cooperative enforcement program allowing DOT personnel to enforce TSA's security training requirements as they conduct their safety inspections. Several commenters suggested TSA coordinate with the owner/operator before an inspection, and one suggested that TSA provide an audit checklist before arriving on the owner/operator's property. Another commenter asked TSA inspectors to undergo safety training before visiting the property. Finally, one commenter suggested TSA consider an audit program for contractors, rather than making the owner/operator responsible for ensuring contractor receives training or otherwise comply with the rule's requirements.

TSA response: As explained in the NPRM, TSA is mandated to: (1) Enforce its rules and requirements; (2) oversee the implementation and ensure the adequacy of security measures; and; (3) inspect, maintain, and test security facilities, equipment, and systems for all modes of transportation.[79] TSA's authority over transportation security is comprehensive and supported with specific powers related to the development and enforcement of security-related regulations and other requirements. Within this broad authority, the agency may assess a security risk for any mode of transportation and develop security measures for dealing with this risk.[80] If TSA identifies noncompliance with its requirements, TSA may hold the owner/operators responsible for the violation and subject to enforcement action, which may result in civil monetary penalties.[81]

Pursuant to its statutory authority and responsibilities, TSA is the sole Federal agency with authority to enforce its regulations. DOT's components do not have authority to enforce TSA's rules and TSA cannot enforce theirs. DHS and DOT, however, do consult and coordinate with each other on security-related issues pursuant to various memoranda of understanding (MOU). To mitigate concerns about duplication of efforts by inspectors, DHS has entered into an MOU with DOT with separate annexes between TSA and the modal components of DOT. These annexes address coordination on regulatory matters.

When appropriate, TSA will coordinate with an owner/operator on inspections. Notice gives the parties to be inspected the opportunity to gather evidence of compliance and to arrange to have the appropriate personnel available to assist TSA. Some inspections, however, can only be effective if TSA's presence is unannounced. TSA must have the flexibility to respond to information, operations, and specific circumstances whenever they exist or develop.

Security concerns are different at different times of the day and on different days of the week. Terrorists may seek to take advantage of vulnerabilities whenever they occur.

[73] *Id.* at 91344.

[74] *Id.* at Table 3, *Explanation of Proposed Terms and Definitions.*

[75] *See* 49 CFR 236.1003.

[76] *See supra,* section II.A.4 for more discussion on the distinction between hosting and contractual relationships and the ramifications for responsibility of providing security training.

[77] *See* sec. 1302(a) of the 9/11 Act. TSA is issuing this rule under the authority of 49 U.S.C. 114.

[78] *See https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf.*

[79] *See* 81 FR 91341, *citing* 49 U.S.C. 114.

[80] 49 U.S.C. 114(f) and (l).

[81] 49 U.S.C. 114(f) and (v).

TSA has the authority to assess the security of transportation entities during all times of the day or night and under all operational situations (including nights, weekends, and holidays). The nature of any given TSA inspection will depend on the specific circumstances surrounding a particular owner/operator at a given point in time and will be considered in conjunction with available threat information.

An audit checklist is unnecessary for this program. Under the rule, owner/operators are required to submit a security training program to TSA for approval. As the regulated owner/operators are the original drafters of the security training program approved by TSA, they should not need a checklist from TSA to inform them of the program's content and requirements. The use of TSA-provided training material does not eliminate the owner/operator's ownership of the program and knowledge of the program's contents. The security training program developed and submitted by the owner/operator to TSA for approval is likely to include additional information provided or developed by the owner/operator to meet all of the curriculum requirements.

Regarding having TSA inspectors undergo safety training prior to visiting a property, TSA's inspectors are properly trained regarding how to safely inspect an owner/operator's property and the importance of complying with official safety-related requirements while on the owner/operator's property. For example, TSA puts its inspectors through a rigorous training program, incorporating classroom and field training, so inspectors are knowledgeable on all aspects related to this regulatory program as well as on safety issues. TSA recognizes the importance of this training to ensure inspectors avoid danger to themselves, to workers on the inspected property, to travelers, and to the inspected property.

Finally, concerning the suggestion that TSA consider an audit program for contractors, in lieu of making the owner/operator responsible for ensuring contractor receives training, TSA applies two important regulatory policies related to responsibilities of contractors. First, contractors performing measures required under TSA's rules are ''authorized representatives'' of the regulated party.[82] As part of its general enforcement policy, TSA consistently holds regulated parties responsible for the actions of their authorized representatives.

Second, authorized representatives and other contractors (and their employees) are also responsible for complying with TSA's regulatory requirements. Under section 1570.7 of this rule, any person may be subject to enforcement action for violations of the rule, including contractors who provide service to owner/operators and the employees of such contractors. As a result, TSA could pursue an enforcement action against the regulated party, the regulated party *and* the contractor as an authorized representative, or against the contractor.

C. Part 1570—General Rules

1. Terms Used in This Subchapter (§ 1570.3)

Comments on definition of ''security-sensitive employees'': In addition to comments of general support for the definition of security-sensitive employee, TSA received a few questions about the term. One commenter sought more information on what defines an employee in a security-sensitive position, specifically asking whether the definition includes a cyber-expert or a frontline engineer staffing a commuter train. Another commenter suggested replacing the term with ''Frontline Employees'' for consistency with the 9/11 Act, finding the term ''security-sensitive'' to be confusing and therefore subject to misinterpretation. Further, this commenter found no risk-based justification for establishing a classification of employees to determine who should receive security training.

TSA response: As discussed in the NPRM, the definition of ''security-sensitive employees'' includes employees who perform functions with a direct nexus to, or impact on, transportation security based on their job functions.[83] Engineers are specifically covered within the job functions identified for 49 CFR parts 1580 (freight railroads) and 1582 (public transportation and passenger railroads). A cyber-expert may be considered a security-sensitive employee based upon specific job functions, such as functions involving control or movement of trains, or because of other cyber-security responsibilities related to the owner/operators security measures in its security plan to protect the integrity of its information systems.

TSA chose the term ''security-sensitive'' for this rule to mirror the term ''safety-sensitive'' used in rules promulgated by DOT. There is no statutory requirement for TSA to specifically use the term ''frontline employee,'' as long as the scope of the rule includes the employees identified in relevant portions of the 9/11 Act, which it does.

Finally, as discussed in the NPRM,[84] TSA applied a risk-based approach to all requirements in this rule, including the definition of security-sensitive employee. The NPRM explained TSA began with an analysis of the employees listed in the 9/11 Act's definitions of ''frontline employees'' who must receive training[85] and then considered whether other employees may also be in a position to spot suspicious activity because of where they work, their interaction with the public, or their access to information. TSA also considered who needs to know how to report or respond to these potential threats. This additional group of employees includes managers, supervisors, or others who perform the function or who so directly supervise the performance of a function that their nexus to the job function is equivalent to the employee.

2. Recognition of Prior or Established Security Measures or Programs (§ 1570.7)

Comments related to use of existing training: Several commenters suggested that TSA should allow use of previous training or programs to satisfy the rule's requirements. The range of these existing programs include training provided under TSA's First Observer™ program and existing railroad security training, which commenters assert meets the intent of the 9/11 Act. Commenters noted that both freight and passenger railroads currently maintain effective security training programs.

Comments on how to use these existing programs varied, including allowing owner/operators to amend their existing programs to make them comply with the rule's requirements; letting currently trained employees be ''grandfathered'' in as long as their training meets the rule's requirements; and a request that TSA determine these existing training programs meet the 9/11 Act's requirements without imposing additional regulatory requirements.

Finally, a commenter expressed concern that owner/operators will be allowed to fulfill the training requirements in a variety of ways, creating unique programs for each system. The commenter noted the

[82] *See* the rule's definition of ''authorized representative'' in 49 CFR 1500.3.

[83] 81 FR 91333 *et seq.*

[84] *See id.* at 61353–61355.

[85] *See id.* at Table 6, *Comparison of security training NPRM proposed categories for ''security-sensitive employees'' to 9/11 Act definitions of ''frontline employees'' who must be trained.*

training requirements may become overly burdensome for employees and employers if an employee must be re-trained every time he or she leaves one transportation operation and joins another.

TSA response: Consistent with requirements of the 9/11 Act, the rule specifically provides for recognition of previous training in § 1570.107.[86] Under this section, owner/operators can use previously provided training meeting or exceeding the requirements of the rule to the extent they can provide documentation of the training and validation this training satisfies the requirements applicable to that employee. The rule also provides owner/operators with the flexibility to use other training programs addressing some or all of the same topics to satisfy the regulatory requirements in §§ 1580.113(c), 1582.113(c), and 1584.113(c).[87]

TSA recognizes that many of the owner/operators to be regulated by this rule have taken voluntary actions to raise their security baseline. TSA applauds these efforts, but also notes that they do not negate the benefits of this rulemaking. The purpose of this rule is to solidify the baseline for those that have already implemented security training programs, and to raise those who have not to a consistent standard across higher-risk operations. To the extent owner/operators established security training programs consistent with the 9/11 Act as a voluntary initiative or implemented use of TSA's First Observer™ program,[88] and continue to provide regular training to their employees, these efforts should significantly mitigate any costs for compliance with the rule.

Finally, the provision on use of previous training, in § 1570.107, also addresses concerns about unique training programs and the impact on employees who change jobs. If the owner/operator can validate the content and timing of the previous training, the rule allows this training to be credited towards satisfying the regulatory requirements. At most, the new employer may need to supplement portions of previous training to address unique aspects of its own TSA-approved security training program. This allows the owner/operator to ensure all of the security-sensitive employees receive training specific to their operations in order to best mitigate security risks.

3. Submission and Approval (§ 1570.109)

Comments on frequency of submitting security training programs to TSA: Two commenters suggested companies should be permitted to submit training plans and curriculum only once to TSA, which TSA would store and review on a yearly basis and make recommended changes based on the current threat.

TSA response: The rule does not impose a specific schedule for owner/operators to submit updates to their security programs, such as an annual update. It does, however, require owner/operators to request to amend their programs if necessary to reflect changes in ownership or permanent changes in operations affecting the security training program or curriculum.[89] For example, a program may need to be updated if the owner/operator replaces equipment resulting in instructions conflicting with the current security training curriculum, or expands operations into a new commodity with different risks, changes personnel structures affecting reporting, or begins operations in a new geographical area. In addition, the final rule narrows the scope of amendments required for changes to security measures or plans. Recognizing an owner/operator's security program may include issues not specifically relevant to the scope of transportation security this rule is intended to address, the final rule includes a list of the specific type of measures and program changes triggering the requirement to request an amendment. TSA may also require owner/operators to amend their plans in the interest of the public and transportation security.[90]

Comments on methods for submitting security programs to TSA: A number of commenters supported submitting training programs to TSA via electronic means, such as in email on a secured password protected platform. One commenter also expressed support for the proposed initial security program submission and approval process, as well as the amendment approval process.

Two commenters, however, raised concerns with this process, claiming it is too rigid and cumbersome to be effective. Commenters noted railroad training programs are robust and adaptable, evolving to address threats and security concerns. To continue to be effective, the commenters advocated that they be allowed to update their programs as needed without TSA approval. They also noted the FRA already oversees railroad security training programs, and TSA inspectors can review the same materials. They noted that given their current process, the NPRM lacked adequate justification for the imposition of a prescriptive process for submission, review, and approval of training programs already in effect.

TSA response: In response to concerns regarding form of submission, TSA intends to allow for electronic submission of required documentation, consistent with SSI requirements. Relating to the need for updating programs, the final rule requires owner/operators to adapt their training materials to address specific threats in the various modes as they emerge. TSA approval is not required for an update unless the changes stay in effect for more than 60 days. For example, an owner/operator may provide additional training to address risks associated with a city hosting a national special security event. If the changes are to stay in effect for more than 60 days, the owner/operator must formally request approval to amend their security program. As the required content for the required security training is general operation security, TSA does not anticipate the TSA-approved security training needing to change significantly in response to a specific threat.

As to the concern about duplication of effort, TSA may accept all or portions of an owner/operator's existing security training. Under § 1570.107, an owner/operator may rely on previous training provided within the stipulated periods for initial or recurrent training, as validated by TSA (based on information submitted by the owner/operator). In addition, the rule provides for owner/operators to rely on training conducted pursuant to other requirements to satisfy the rule's security training requirements.[91] In fact, the rule specifically references training required by FRA.[92] In reviewing material prepared for other requirements, TSA will determine whether the material adequately addresses security training from TSA's perspective and reduces the risk of a terrorist-related attack on the transportation. As previously noted, TSA mitigates concerns about

[86] *See id.* at 91347 for the discussion on this topic in the NPRM.

[87] *See id.* at 91361–91362.

[88] The First Observer™ program, previously known as Operation Secure Transport, has been in use for highway motor carriers (OTRB owner/operators) and covers the Observe, Assess, and Respond security training components required by this rulemaking. TSA credits those OTRB owner/operators who have used the First Observer™ program in its RIA (full description in Section 1.5 of the Final RIA).

[89] *See* § 1570.113 and discussion in section IV.B.1.

[90] *See* § 1570.115 and discussion in section IV.B.2.

[91] *See* §§ 1580.113(c), 1582.113(c), and 1584.113(c).

[92] *See* §§ 1580.113(c) and 1582.113(c).

duplication of inspections, through the annexes to the DHS/DOT MOU. These annexes address distinctions between TSA's focus on security and DOT's focus on safety, as well as coordination on regulatory matters between TSA and the relevant modal components of DOT.

Finally, regarding the prescriptive process requirements, TSA reviewed all requirements in this rule to identify any options to reduce the burden without undermining the rule's effectiveness or conflicting with requirements in the 9/11 Act. The 9/11 Act specifically requires submission of the training programs to DHS for approval and regular updates.[93] TSA believes the submission and approval requirements in § 1570.109 are consistent with this statutory requirement, provide clear instruction on how this requirement is to be met, and ensure consistent application of the rule's requirements.

4. Implementation Schedule (§ 1570.111)

Comments on initial security training: Several commenters advocated for the proposed accumulated grace periods, ranging from 90 to 180 days, to allow recently hired employees to work before they complete the training requirements. One commenter suggested abandoning the accumulated days concept and replacing it with a requirement for all employees to receive security training no later than 90 days after beginning employment. One commenter suggested a method for calculating date: A day should be based on full-time employment, with each 8-hour period worked counting as one day. Regarding contractors, the same commenter suggested the training responsibility should rest with the contracted company.

Comments also addressed how to regulate temporary and/or part-time employees. One commenter suggested all drivers, whether employees or contractors, should be trained. Another commenter explained ''pooling agreements,'' which allow or require employees from other companies to operate their equipment, and noted these arrangements should be covered in the final rule.

TSA response: While TSA appreciates concerns regarding the implementation schedule for initial training, the 60-day requirement is set by the statute. As noted in the NPRM, the 9/11 Act requires initial training within the first 60-days of employment for new employees or for those transitioning to a covered job function (as identified in Appendix B to parts 1580 (freight rail), 1582 (PTPR), and 1584 (OTRB).[94] TSA is not adopting the suggestion of a day equaling an aggregated 8-hour period. TSA's intent with this rule is to ensure employee's that are regularly positioned to identify and respond to security threats are prepared to do so. TSA does not believe that this priority is served by hourly calculations to determine what constitutes a day.

As to contractors, TSA consistently applies a policy requiring regulated parties to accept responsibility for their contractors, including employees operating under pooling agreements. Any person working for an owner/operators within the scope of applicability, performing a security-sensitive position—without regard to primary employer or full/part-time status—must be trained. In other words, a pooling agreement does not mitigate the need for security training. The impact of this policy is more fully discussed under comments related to 49 CFR part 1503.

Finally, TSA is not changing the aggregated employment requirement in § 1570.111(4) nor the requirement for employees (whether intermittent or contract) to be trained no later than the 60th day of aggregated employment performing a security-sensitive function. This requirement ensures these employees are trained after they are in a position with a particular owner/operator long enough to gain awareness of the operations necessary to determine when there is an anomaly that could constitute a threat.

In response to the comment about all drivers (presumably of OTRBs) being required to receive training, TSA is limiting it to individuals with a commercial driver's license to focus on those with a nexus to security, in other words, those likely to operate a bus to, through, or from a high-risk location, rather than employees moving a bus across a yard. While TSA is not currently requiring all drivers to receive the security training, this does not prevent owner/operators from voluntarily providing the security training required for security-sensitive employees to a broader population of employees.

In addition, TSA is developing training materials that can be consistently used across a particular mode. Use of this material, coupled with the ability to use previous training, will minimize the burden of ensuring employees in pooling agreements received adequate training. Owner/operators can rely on the TSA-provided material to address most of the requirements and limit their operation-specific training to procedures unique to their operation, such as points of contact to report security concerns and emergencies.

Comments on recurrent security training: TSA received a variety of comments on recurrent training. Some commenters generally supported annual recurrent training. Other commenters stated they should have flexibility to self-determine the training schedule for their employees, as opposed to an adhering to a ''one size fits all'' approach. Some commenters expressed concern with the time frame due to cost constraints and the practicality of training employees while simultaneously maintaining service. These commenters suggested longer time periods between training, such as two or three years. One commenter highlighted the safety requirements in FRA's rules, which require training every three years.

TSA response: TSA considered options for recurrent training both before proposing the requirement in the NPRM and in consideration of comments submitted on the NPRM. TSA continues to believe in the importance of recurrent training to meet the purpose of the rule, but is adjusting the frequency of training in consideration of the comments. The final rule requires recurrent training once every three years. If, however, the owner/operator modifies its security program or plan and those changes affect the responsibilities of specific security-sensitive employees, based on their position or function in relation to security program or plan requirements, the affected employees must receive recurrent training to address the changes within 90 days of implementation of the revisions. This change is consistent with the requirements for hazardous materials employees under 49 CFR 172.704.[95] The recurrent training requirements are discussed in more detail in section II.J.2.

5. Recordkeeping and Availability (§ 1570.121)

Comments: Two commenters said the proposed 5-year record-keeping requirement would be excessive in duration, costly and burdensome in administration, and unjustified by any risk-based factors. As an alternative, they suggested owner/operators should only be required to retain training from

[93] 9/11 Act sections 1408(d), 1517(d), and 1534(d).

[94] *See* 81 FR 91347.

[95] In addition, TSA notes that it may order modifications to a security program or plan, or order additional training, as necessary. *See, e.g.,* 49 U.S.C. 114(l).

the past three years (assuming TSA adopts a 3-year training requirement).

TSA response: Within the context of an annual recurrent training requirement, TSA considered modifying the record retention period based on the comments as three years would provide adequate records of previous training. The change, however, to recurrent training on a three-year cycle necessitates maintaining the 5-year retention schedule in order to ensure that the owner/operator can provide adequate representation of previous training consistent with recurrent training requirements as well as any training based on modification to the owner/operator's security program or plan.

6. Security Coordinator (§ 1570.201)

Comments on security coordinator availability: Two commenters suggested changes to the security coordinator requirements specifically for railroad companies. First, they suggested TSA only require affected railroads to maintain a 24/7 communications capability to ensure TSA can reach the rail security coordinators and designated representatives for the stated purpose of receiving intelligence information and coordinating on security practices and procedures.

Second, there was one objection to the proposed requirement for freight railroad operators to name rail security coordinators (RSC) ''accessible to TSA on a 24-hour a day, 7-day a week basis.'' The commenter suggests modifying this proposal to require the railroad to ''maintain a 24/7 communications capability to ensure TSA can reach the RSCs and designated representatives for the stated purpose of receiving intelligence information and coordinating on security practices and procedures.''

TSA response: First, TSA is reorganizing the location of the RSC requirements promulgated in 2008, moving the requirements from 49 CFR part 1580 to part 1570 (§§ 1570.201 and 1570.203) and expanding applicability of the existing RSC requirement to include bus operations of public transportation systems and OTRB owner/operators within the scope of the rule's applicability. TSA neither proposed nor is adopting any modifications to the RSC requirements as they apply to railroads and the requirement regarding 24/7 accessibility of security coordinators.

It is critical for security coordinators to be ''accessible to TSA on a [24/7] basis'' rather than accepting ''a 24/7 communications capability [that] can reach the RSCs.'' Although most communication between TSA and security coordinators may be routine, these individuals are intended to serve key roles in times of heightened and specific security threat and incident. During such periods, immediate communication with the security coordinators may be required to prevent or mitigate loss of life or severe harm to transportation security. TSA believes the requirement for security coordinators to be accessible to TSA on a 24-hour a day, 7-day a week basis is amply justified by commonly accepted principles of emergency and security management. If TSA needs to convey extremely time-sensitive security information to a regulated party, particularly in situations requiring frequent information updates, the information exchange benefits if there is continuity in participants. The security coordinator must be in a position to understand security problems, raise issues with corporate leadership, and recognize when emergency response action is appropriate. If the contact changes every time TSA makes a call, the loss of continuity will undermine the effectiveness of the communication.

Comments on citizenship requirement for security coordinators: Two commenters stated disclosing citizenship status is unnecessary and should not be required. One of the two commenters suggests TSA should recognize Canadian government security clearances in lieu of requiring RSC to be citizens of the United States.

TSA response: The rule does not require a rail security coordinator to be a citizen of the United States. It does however, require each owner/operator to report the citizen status of individuals it intends to put forward as its RSC under § 1570.201(d). This requirement is necessary to meet the 9/11 Act requirement that security coordinators be U.S. citizens unless TSA determines it is appropriate to waive the requirement ''based on a background check of the individual and a review of the consolidated terrorist watchlist.'' [96] By providing this information up front, TSA can initiate any additional actions necessary to comply with this requirement.

7. Reporting Significant Security Concerns (§ 1570.203)

Comments on mandatory reporting requirement, scope of reporting, and form of reporting: Several commenters opposed a mandatory reporting requirement. A few argued the requirements would open up their companies and employees to liability should an incident occur and an earlier warning action was not observed. Several other commenters specifically opposed the 24-hour proposed time limit, stating it was too short, and some transit agencies may not know what the threat is in that amount of time.

Commenters also suggested TSA authorize electronic reporting of significant security concerns to meet the reporting requirements in § 1580.203. These commenters noted the rail industry has developed an electronic reporting capability and demonstrated its effectiveness in three industry-wide exercises.

Finally, a few commenters asked for additional clarity regarding what ''significant security concern'' entails, and one asked for a list of examples. One commenter specifically suggested TSA harmonize its definition of ''security threat'' with the FRA's requirement in 49 CFR part 239. Several commenters suggested streamlining the requirements.

TSA response: As with the security coordinator requirement, TSA is reorganizing the location of the reporting significant security concerns requirements promulgated in 2008 (which were at 49 CFR part 1580), placing the requirement in part 1570 to expand its applicability to OTRBs and bus operations of public transportation system companies within the scope of the rule's applicability. As proposed in the NPRM, TSA is making three primary changes to the current requirement through this final rule. These changes affect all owner/operators required to report, but results in a reduced burden for rail operators previously required to report. First, the rule modifies the current requirement to report *immediately,* to allow *up to 24 hours* to report significant security concerns. TSA is providing a period of up to 24 hours to report the information for two reasons: (1) If there is an emergency, the immediate priority is to notify and work with first responders, not call TS, and (2) TSA is aware the quality of information provided is improved when owner/operators have an opportunity to review the information and ensure it constitutes a valid significant security concern consistent with the description of activities in Appendix A to part 1570 before it is reported. TSA believes 24 hours is an adequate period for this process to work effectively. If more time is granted, the information may be too stale to be of benefit to TSA or its other stakeholders.

Second, TSA is modifying the existing requirement to allow for electronic reporting. The current rule requires reporting to be made by telephone. With

[96] *See* 9/11 Act sections 1512(e)(2) and 1531(e)(2).

this final rule, TSA is expanding the requirement to allow for other methods prescribed by TSA. TSA will communicate these methods directly to security coordinators to avoid a situation where a phone number or email address may become outdated based on changes or requirements beyond the scope of this rulemaking.

Third, as noted in the NPRM and discussed in section III.C, TSA is including in the final rule a table that identifies categories of incidents and provides detailed descriptions.[97] These incidents are modified from the requirements promulgated in 2008 to align with other standards, including those mentioned by commenters, and recommendations from the Government Accountability Officer (GAO).

D. Subpart B—Security Programs

1. Security Training Program General Requirements (§§ 1580.113, 1582.113, and 1584.113)

Comment on content creation: TSA received several comments regarding responsibility for creating training content. TSA also received questions concerning who will conduct training and the training format, including recommendations for TSA to consider video training, in-classroom, and/or field training. Another commenter suggested putting a one-hour cap on course length. One commenter suggested an outside entity, not TSA, should provide oversight for compliance with the training. Several commenters also suggested TSA should require transit systems, rail carriers and OTRB operators to seek the input of employees and union representatives as they draft their training plans, which would ensure the plans consider individual circumstances and are effective in promoting transportation security.

TSA response: Rather than putting limits on curriculum development, the rule requires owner/operators to submit their security training programs to TSA for review and approval. While the burden is on owner/operators to develop and provide the training, the rule neither prescribes how the content is to be created nor dictates how it is to be provided. The flexible requirement is an intentional effort to address the varied operational issues for owner/operators required to provide training. For example, larger owner/operators may determine it is more cost-effective to incorporate the training required by this rule into existing training provided in a classroom. For smaller operators, web-based training may be easier.

To address this variety, the rule requires owner/operators to develop and implement a security training program meeting the requirements of the relevant subparts and ensures the standards are met by requiring the program to be submitted to TSA for review and approval of the curriculum (including lesson plans, objectives, and modes of delivery) and method for measuring effectiveness.[98] TSA is unwilling to put a cap on the requirement. Based on the security awareness training TSA requires for its own employees as well as its work and discussions with experts on content development, TSA assumes adequately addressing all of the required elements will take approximately one hour.

TSA is committed to providing maximum flexibility within the constraints of the 9/11 Act's requirements and needs of regulatory compliance. To support compliance, TSA intends to provide complimentary training material satisfying many of the rule's requirements. If owner/operators choose not to use this material, they will need to develop a *full* curriculum to be approved by TSA. If they do use it, they may still need to submit additional material for any portion of the required training (based on their unique operations) not covered by the TSA materials. As a result, the rule provides a process balancing flexibility (for owner/operators to develop a program specific to their operational environment) and TSA's need to ensure training programs meet the rule's purpose.

TSA does not agree with suggestions for third-parties (not TSA) to oversee the curriculum development and training. In light of the flexibility given for curriculum development, TSA must ensure the minimum requirements of the rule are met in order to satisfy both the mandate of the 9/11 Act and TSA's intent for this rule to provide a consistent baseline of security training across higher-risk operations. TSA's subject matter experts for the modes of operation covered by this rule will lead this review and approval process.

TSA agrees the materials should be relevant to the operational environment and the employees who work within that environment. Like other aspects of curriculum development, the rule gives owner/operators the flexibility necessary to meet this objective without imposing a prescriptive requirement. Similarly, the rule does not prohibit owner/operators from consulting with relevant parties or developing programs appropriate for their operational environment.

Comment on size of train crew: One commenter noted that a two-person minimum crew in train cabs is vital to defending national security. Their concerns reflected current operational requirements, such as monitoring of computer screens rather than monitoring conditions outside of the train (such as the track).

TSA response: The purpose of this regulation is to ensure employees performing security-sensitive functions receive adequate training. Staffing requirements for train operation are beyond the scope of this rulemaking.

Comments on effectiveness of security training: The rule requires owner/operators to include in their security training programs a method for evaluating the effectiveness of the program.[99] A few commenters suggested ways to ensure the training is effective and applicable to real-world situations. Suggestions included having businesses put up a poster as a general reminder of the material covered in the class, creating incentives (monetary or time-off awards) to completing training, and ensuring class is engaging and not only a lecture in a classroom. Another suggestion was to integrate randomized written tests or drills of the covered material, of which successful completion could warrant an award. Comments included suggestions for training to be conducted in a classroom, citing two benefits of classroom training: (1) Allows employees to ask questions and learn from questions and discussions and (2) allows instructors to work with employees through a variety of scenarios, which would include teaching how to look out for and spot various security threat and explain the various roles each employee serves in responding to these threats. One commenter asked whether the training could be incorporated into ''Entry Level Driver''-training, and also suggested an online ''train the trainer'' course.

Commenters were divided on the question of whether the training's effectiveness should be documented through testing. Several commenters stated that classroom testing should be augmented by field testing. Others suggested no testing should be required. Several commenters suggested that TSA incorporate efficacy standards or incentives for public transportation agency employees. As an alternative, a number of commenters opposed any kind of proficiency testing on the training course material.

[97] *See* Appendix A to part 1570. *See also* 81 FR 91351–91353.

[98] *See* §§ 1580.113(b)(6), 1582.113(b)(6), and 1584.113(b)(6).

[99] *See* §§ 1580.113(b)(9), 1582.113(b)(9), and 1584.113(b)(9). *See also* discussion at II.K.

TSA response: TSA is requiring the owner/operator to describe the method to be used for measuring effectiveness of security training and will conduct inspections to ensure the approved method is being used, as part of implementing the TSA-approved security training program. While TSA appreciates the information provided by commenters for measuring the effectiveness of training, TSA has decided not to dictate which method must be used. As part of its commitment to recognizing the many unique operational environments for owner/operators subject to this regulation, as well as the commitment to balance maximum flexibility with effective security, TSA is not requiring a specific method for measuring effectiveness.[100]

TSA recognizes that pre- and post-testing in a classroom setting is an efficient way to determine the effectiveness of training. TSA also acknowledges, however, that, other methods of documenting the effectiveness of training exist, which may be preferable for some employees and/or circumstances. Therefore, TSA is not specifying a particular type of testing or other method for determining effectiveness, but will use the owner/operator's TSA-approved standard for measuring effectiveness when inspecting an owner/operator's training documentation to verify that each employee who must be trained has received the required training and that the owner/operator has determined that the training is effective.

2. Security Training and Knowledge for Security-Sensitive Employees (§§ 1580.115, 1582.115, and 1584.115)

Comments on security training knowledge requirements: TSA received varied comments on the required security training curriculum content requirements. The comments ranged from asserting that the scope of the training content is overly broad to proposing additional training requirements to be added to the rule.

One commenter, concerned that the scope is too broad, suggested training beyond awareness observation and reporting may be excessive and counterproductive to the safety and convenience of passengers. The commenter recommended that security training requirements not exceed the parameters of the employee's unique tasks or working environment.

Finally, some commenters wanted topics added to the curriculum. Two commenters suggested the training focus on civil liberties, and integrate community policing principles. Other proposed topics included how to respond to an attack, high-jacking, and/or kidnapping scenario; self-defense training; specified training on high-risk events; training on accessing and interpreting situations; and development of communication skills.

Commenters suggested the training address issue of civil rights and liberties, expressing concerns about training employees to identify individuals as threats based on their socioeconomic status. One commenter specifically cautioned against enabling transit security personnel to profile riders based on race or religion, and suggested personnel should first be trained to respect rights of all individuals, and should also be trained in effective measures not involving ''stop and frisk,'' or similar measures.

TSA response: TSA believes the required security-training topics (covering prepare, observe, assess, and response) will provide a baseline of security awareness to enhance the overall safety and security of passenger and cargo transported by rail and highway. This type of security awareness does not inconvenience passengers or undermine their safety. It does, however, enhance passenger security. Furthermore, nothing in the rule empowers employees to engage in racial profiling or conduct police operations. TSA will not approve a training curriculum encouraging employees to conduct racial profiling or report threats based on socioeconomic status.

Finally, the regulatory requirements for training content provide flexibility to owner/operators to develop programs appropriate to their operational environment, including known threats and vulnerabilities. As a result, training may include how to identify threats such as a potential hijackers and how to prepare and use the required training during high-profile events (including appropriate communications with the public and first responders). The requirements of this rule will enhance such targeted, optional training. The rule's requirements will result in employees possessing an understanding of the norm for their operational environment, the skills and knowledge necessary to identify anomalies indicating a potential threat, and the capability to respond appropriately.

Comments on training to satisfy regulatory requirements: Several commenters requested more specificity regarding what type of training will satisfy the curriculum requirements, including a list of examples. One commenter asked for guidance on what type of training will satisfy the curriculum requirement concerning ''defending oneself.''

TSA response: In the past, TSA has worked with the relevant associations and FEMA to identify training to address specific security needs and anticipates continuing to do so as it relates to the requirements in this rule. In addition, TSA has partnered with national associations and industry to cooperatively develop security training curriculum and programs. While TSA does not intend to endorse specific third-party training programs owner/operators may submit these programs to TSA as part of their security training programs. TSA will assess all submitted programs to ensure compliance with the rule's requirements before approving the training program. As to the comment on providing more information on ''defending oneself,'' the rule does not require training on how to use self-defense devices or other protective equipment provided by the employer. TSA assumes the employer's standard employee training will address these issues at the time the equipment is provided (one commenter noted the Occupational Health and Safety Administration (OSHA) requires employees to receive training in the use of (PPE) required by their job functions).

Comments on impact of TSA-developed security training materials: One commenter suggested that TSA develop an annual course based on current threat and intelligence rather than requiring companies to create annual plans for TSA approval. Similarly, several commenters suggested that TSA create a baseline curriculum, such as a video, that would meet the regulatory requirements. One commenter suggested that companies could voluntarily submit supplemental training that exceeds the recommended baseline training that is specific to their mode. One commenter, however, specifically stated that TSA's First Observer™ training materials are inadequate.

TSA response: This rule does not require owner/operators to submit updated plans every year. Updates, or amendments, are only required for specific reasons, as discussed in section IV.B.

In regard to the comments regarding use of First Observer™, TSA notes that the First Observer™ program most familiar to regulated parties was created primarily for highway and motor carrier professionals. While TSA assessed that First Observer™ covers three of the required training elements for OTRB owner/operators, the program was not created to specifically address this rule

[100] For further discussion, *see* 81 FR at 91361.

nor was it meant to be applicable to all surface modes of transportation.

At the time the NPRM was published, TSA anticipated expanding the First Observer™ program to incorporate additional training material. Since publication of the NPRM, however, TSA initiated development of new materials to address three of the required training program components (Observe, Assess, and Respond) that are relevant to all owner/operators within the three covered modes.[101] While these videos are a new product intended to specifically align with the rule's requirements, they build upon previous training developed by TSA under First Observer™ and other transportation security-related training programs. TSA adapted this previously developed information, and supplemented it as necessary, to ensure the videos address as many of the required training elements as can be met through a one-size fits all training video. These materials may eventually be placed under the First Observer™ umbrella, but will not be the same as the original program.

As noted in the NPRM, use of TSA-developed and provided material is optional. TSA developed these materials to further reduce the burden of compliance to owner/operators with a resource they *may* use to meet a majority of the security training requirements under this rule. These videos will be made available to all of TSA's surface stakeholders.

TSA is aware that not all owner/operators will choose to use TSA-provided material, particularly if they are incorporating their training into existing training programs to meet other Federal, state, or local training requirements. Owner/operators may need to develop and/or provide supplemental material to ensure the training provided meets all of the training requirements, specifically reflecting nuances within the operations of a particular owner/operator or a particular sub-set or location of these operations. This additional information must be identified and included in the security training program submitted to TSA. As the videos use is not mandatory, the economic analysis does not account for them when estimating costs of compliance.

[101] The ''Prepare'' element of the required training curriculum is, by its nature, specific to each the operations of each owner/operator covered by the rule. As such, this element cannot be addressed in material intended to be applicable to multiple owner/operators.

E. Freight Rail Specific Issues

1. Applicability of Security Training Requirements (§ 1580.101)

Comments: Several commenters expressed concern related to the designated list of HTUAs in Appendix A to part 1580. One commenter believed the training is necessary for all frontline employees, not just those employed by higher-risk operations. Another noted that improving security at some locations may result in terrorists redirecting their operations to softer targets not covered under the rule. The commenter suggested the rule should require security training at all transportation locations. The commenter specifically recommended that the rule cover freight, passenger rail, and public transit systems.

TSA response: As discussed in the NPRM, TSA's risk-based determinations for applicability are consistent with the focus of the 9/11 Act's requirements on higher-risk operations.[102] This risk-based focus is reflected in the statutory requirement for the training to be provided to frontline employees, not all employees, and placing the security training requirements within the context of a broader security program focusing on higher-risk operations.

While hardening one target could make those with nefarious intent believe that other targets are more vulnerable, the threat (an adversary's intent and capability) is only one of the critical factors affecting risk (which also includes vulnerabilities and consequences). The risk analysis underlying the applicability for freight railroad is heavily weighted to address concerns regarding the vulnerabilities and consequences. TSA determined the highest risk freight railroads are those designated as Class I, based on their revenue and the Nation's dependence on these systems to move both freight in support of critical sectors and passengers. All Class I railroads must provide security training. Similarly, some shortlines (also known as Class II or Class III railroads) are higher-risk because of what they transport and where they transport it. As noted above, and in the NPRM, certain materials have a higher-risk associated with them based on the potential consequences should they be released.[103] The likelihood of catastrophic consequences is greater in HTUAs. By reducing the vulnerability through increased security training, the rule's applicability is intended to reduce the risk for these systems without increasing the risk for others. Finally, TSA encourages owner/operators not within the scope of the rule's applicability to use the regulatory requirements as guidance for voluntarily implementing a security training program for its security-sensitive and other employees, whether by using TSA-developed programs or through its own training. These owner/operators may contact TSA through the numbers and addressed identified in under **FOR FURTHER INFORMATION CONTACT**, or through modal associations (with whom TSA regularly interacts).

[102] *See* 81 FR 91355 *et seq.*

[103] *See id.*

2. Chain of Custody and Control Requirements (§ 1580.205)

Comments: Two commenters asserted threat assessments indicate freight railroads face a lower terrorist threat. The commenters concluded the transfer of custody procedures should only apply at elevated or imminent terrorism levels.

TSA response: TSA understands this comment to be about the chain of custody requirements currently required by 49 CFR 1580.107 and not this rule's requirements to provide training on the chain of custody procedures employed by the railroad. For the underlying chain of custody requirements, this rule merely relocates the requirement within the CFR; TSA did not propose modifying them. TSA thus considers these comments pertaining to substantive changes to the chain of custody requirements as beyond the scope of this rulemaking. Consistent, however, with the requirements of Executive Order 13777, *Enforcing the Regulatory Reform Agenda* (Feb. 24, 2017), TSA is addressing this comment as a suggested revision to existing regulations.

Under 49 U.S.C. 114(l)(3), TSA is required to consider the potential impact on security before it rescinds or revises a regulatory requirement. Transfer of custody requirements are intended to prevent access by unauthorized persons to railcars loaded with certain chemicals or materials may constitute an immediate threat to life or health if released into the environment. TSA does not agree that transfer of custody procedures should only apply to elevated or immediate threat risk. The state of the terrorism alert level is not related to the need to deny unauthorized persons access to railcars loaded with hazardous materials; unauthorized persons must be denied access to such railcars at all times. Terrorism alert levels are increased when there is reason to believe a heightened threat of an attack exists or may exist. Accessible freight cars containing hazardous materials may be

used to mount an attack spontaneously, without elaborate planning or premeditation on the part of the attacker, and therefore without warning or reason to elevate the threat level in advance of the attack. Current ''chain of custody'' requirements accomplish this objective and are retained in the final rule.

F. Public Transportation and Passenger Railroad Specific Issues

Comments: Several commenters questioned the scope of the rulemaking in relation to PTPR. Commenters specifically questioned TSA's criteria for identifying the current PTPR systems, and asked whether TSA will identify additional PTPR systems in the future. One commenter urged TSA to reconsider limiting the applicability to 46 systems rather than all PTPR systems, as the cost-savings is far outweighed by the cost-effectiveness achieved by meaningful training of all frontline transit employees in security-sensitive positions. One commenter asked if the Federal Transit Administration's (FTA's) impending repeal of 49 CFR part 659 would mean only TSA's identified ''higher risk'' PTPR systems will have security training requirements, vulnerability assessments, and security planning requirements after April 15, 2019.

TSA response: As noted above, TSA's risk-based determinations for applicability are consistent with the 9/11 Act's requirements regarding higher-risk operations. This focus on risk is reflected in the statutory requirement for training frontline employees, not *all* employees, and placement of the security training requirements within the context of a broader security program required to focus on higher-risk operations. In questioning TSA's criteria for its determination, the commenter provided no specific information regarding TSA's perceived failures nor provided alternatives. If TSA decides to expand the rule's applicability to additional systems, it would do so through appropriate rulemaking procedures consistent with TSA's statutory authorities and rulemaking requirements.

TSA cannot confirm the rule will continue to be as cost-effective if the number of PTPR systems is expanded. In the NPRM and Final RIA, TSA performed an alternatives analysis (Section 5.2 of the Final RIA), in which one of the alternatives expanded the scope of affected PTPR owner/operators from 47 (46 PTPR systems + Amtrak) to 253. This alternative would result in the costs of compliance for the PTPR industry to increase from $2.44 million to $14.93 million (both annualized and discounted at 7 percent).[104] It seems unlikely that expanding security training to an additional 206 owner/operators, to include operations not considered higher-risk, will yield a corresponding reduction in risk. As previously noted, TSA encourages owner/operators not covered by the rule's applicability to use the regulatory requirements as guidance for voluntarily implementing a security training program for its frontline employees, whether by using TSA-developed programs or through its own training.

Finally, the nexus between the FTA's requirements and this rule are more fully discussed in the NPRM.[105]

G. OTRB Specific Issues

1. Definition of Security-Sensitive Employees (§ 1584.3 and Appendix B to Part 1584)

Comments: Two commenters expressed concern that bus companies do not always know in advance exactly which buses will be used for which service. One of the commenters suggested it would be easiest for their company if all drivers take part in mandatory training, regardless of their normal scheduled route, as there is potential for a driver to be transferred to a different assignment at the last minute. Another commenter cautioned the rule may cause confusion as to which employees of an operation should be trained, and asked for clarification whether an operator should only train front line employees servicing identified destinations. The commenter explained a scheduled service operator may offer charter, shuttle bus, or other transportation services, in addition to fixed-route service to areas that are outside the UASI areas.

TSA response: To address the request for clarity, TSA recommends owner/operators first determine whether they have operations placing them within the scope of the rule's applicability, *i.e.,* whether the owner/operator provides fixed-route service to, through, or from one of the areas identified in Appendix A to part 1584. If so, the owner/operator must provide security training to all of its security-sensitive employees. The question of which employees receive training is not based on where the employee's job takes them, but what their job requires them to do. Thus, all employees who have a commercial driver's license and operate an OTRB for the owner/operator must receive security training, not just those who drive an OTRB to, through, or from an identified area.

The comments provided conflicting opinions on whether requiring all security-sensitive employees to receive the training, regardless of where the individual operates, is necessary. TSA is requiring that all security-sensitive employees must be trained, but notes that owner/operators may request alternative measures under the procedures in § 1570.117.

2. Applicability (§ 1584.101)

Comments on threat: One commenter disagreed that vehicle borne improvised explosive devices (VBIED) are the greatest and most likely attack risk, citing recent terrorism-related incidents involving vehicle ramming.

TSA response: Within the context of the 9/11 Act's mandate for TSA to require OTRB owner/operators to provide security training to their employees, TSA's risk analysis focused on what risks were greatest for OTRB, not all forms of motor vehicles. To the extent the commenter is suggesting use of an OTRB for vehicle ramming is greater than the risk of using an OTRB as a VBIED, the distinction would have no impact on how TSA uses its risk analysis to determine applicability as the vulnerabilities and consequences for OTRBs are similar. To the extent the commenter is referring to other types of motor carrier-related threats, TSA notes that security awareness training is a valuable countermeasure against vehicle ramming attacks. Because large commercial vehicles can do more damage in a ramming attack, teaching large vehicle operators to be more sensitive to and aware of possible hijacking or other attempts to procure their vehicle can mitigate losses and damages.

Comments on applicability: Several commenters expressed concern with the scope and applicability of the rule. One commenter agreed with the definition of ''higher risk'' and their application to the rule, but urged TSA to ensure DHS provides consistency throughout all its components regarding ''the factors that could make an OTRB a potential target.'' One commenter suggested that UASI may be ''over kill,'' and suggested only 10 areas. Another expressed concern that as UASI areas are re-determined annually, the prioritized locations could change frequently, which would result in an undue burden on operators and foster soft targets as resources are shifted to address new threats. Finally, commenters expressed concern that the rule may create ''soft targets'' which could be exploited by terrorists.

[104] *See* Final Rule RIA, tables 40 and 91 for total costs to PTPR in the preferred alternative and Alternative 2 (expanded population), respectively.

[105] *See* 81 FR at 91365.

TSA response: As discussed in the NPRM,[106] TSA's risk-based determinations for applicability are consistent with the focus of the 9/11 Act's requirements on higher-risk operations. This is reflected in the statutory requirement for the training to be provided to frontline employees, not *all* employees, and placing the security training requirements within the context of a broader security program that focuses on higher-risk operations.

While hardening one target could make those with nefarious intent believe that other targets are more vulnerable, the threat (an adversary's intent and capability) is only one of the critical factors affecting risk (which also includes vulnerabilities and consequences). The risk analysis underlying the applicability for OTRB is heavily weighted to address concerns regarding the vulnerabilities and consequences, including the vulnerability associated with scheduled service and the consequences should an attack occur in highly populated urban areas.

Because the risk involving an OTRB as a VBIED is primarily to the targeted urban area, TSA relied on a risk model developed by DHS to determine highest risk urban areas for the UASI grant program. This model has been approved by the Secretary of Homeland Security for calculating the relative risk of urban areas in order to inform UASI allocation determinations.[107] As with PTPR, TSA drew the line for applicability where there is a natural and significant break in the funding allocations as informed by the risk methodology.

As to concern about the impact of future changes to UASI designations, that concern is misplaced. While TSA used the UASI designations to develop its applicability determination, the term UASI is not used in the applicability. Instead, the rule applies to those providing fixed-route service to, through, or from one of the areas identified in Appendix A to part 1584. The table in this appendix includes specific counties to avoid any potential confusion regarding applicability.

Finally, TSA does not believe the regulation creates soft targets. By reducing the vulnerability through increased security training, the rule's applicability is intended to reduce the risk for these systems without increasing the risk for others. Finally, TSA notes that it encourages owner/operators not covered by the rule's applicability to use the regulatory requirements as guidance for voluntarily implementing a security training program for its frontline employees, whether by using TSA-developed programs or through its own training.

H. Comments Beyond Scope of Rulemaking

TSA received several comments regarding issuance of self-defense devices, such as tasers and mace, ranging from suggesting that we require employers to issue them to suggesting that we prohibit it. Either suggestion is beyond the scope of this rulemaking. The comment indicating that OSHA mandates employee training in the use of PPE, if required by their job functions, has already been noted.

VIII. Rulemaking Analyses and Notices

A. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) requires Federal agencies to consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA sec. 3507(d), obtain approval from the OMB for each collection of information it conducts, sponsors, or requires through regulations.[108]

OMB has approved a related information collection request for contact information for RSCs and alternate RSCs, as well as the reporting of significant security concerns by freight railroad carriers, passenger railroad carriers, and rail transit systems.[109]

This final rule, however, contains new information-collection activities subject to the PRA. Accordingly, TSA has submitted the following information requirements to OMB for its review. The Supporting Statement for this information collection request is available in the docket for this rulemaking.

Title: Security Training Programs for Surface Mode Employees.

Summary: This final rule requires the following information collections:

First, owner/operators identified in 49 CFR 1580.101, 1582.101, and 1584.101 are required to submit a security training program for security-sensitive employees that meets the requirements of subpart B of 49 CFR part 1580, subpart B of 49 CFR part 1582, and subpart B of 49 CFR part 1584. Additionally, they are required to submit a request to amend their security training program if certain changes are made to their operations or if notified by TSA that an amendment is necessary. For purposes of its burden estimates, TSA assumes such modification will occur every three years.

Second, the public transportation bus systems and OTRB owner/operators to whom the final rule applies would be required to obtain personal and contact information from their designated security coordinator, and alternate, and submit such records to TSA.

Third, respondents would be required to retain individual training records on security-sensitive employees at the location(s) specified in each respondent's respective security training program, and make such records available to TSA upon request.

Fourth, the public transportation bus systems and OTRB owner/operators to whom the final rule applies would be required to report significant security concerns, which includes incidents, suspicious activities, and/or threat information.

Use of: This information will be used to support the implementation of this final rule, including to TSA determinations that security training programs satisfy the requirements in this final rule. Recordkeeping requirements are necessary for TSA to verify employee training is in compliance with the final rule. Security coordinator information supports respondent communications with TSA concerning intelligence information, security related activities, and incident or threat response with appropriate law enforcement and emergency response agencies. The reporting of significant security concerns supports the analysis of trends and indicators of developing threats and potential terrorist activity.

Respondents (including number of): The likely respondents to this information collection are the owner/operators of covered surface modes, which are estimated to incur approximately 579,070 responses over the next 3 years (including 145,731 freight railroad responses; 254,754 PTPR responses; and 178,586 OTRB company responses), which amounts to an average annual cost of $0.93 million.

Frequency: TSA estimates that following initial submission, security training programs would need to be periodically updated as appropriate. Security training records would need to be updated after each training occurrence. Security coordinator information would need to be updated as appropriate. Significant security concerns would be reported as they occur. TSA estimates inspections for

[106] *See* general discussion on applicability, *id.* at 91355 *et seq. See also* OTRB specific discussion, *id.* at 91358 *et seq.*

[107] As the risk methodology relies upon SSI, it is not available to the public.

[108] Public Law 96–511, 94 Stat. 2812 (Dec. 11, 1980), as codified at 44 U.S.C. 3501 *et seq.*

[109] *See* OMB Control No. 1652–0051.

compliance would occur at a rate of one inspection per year per owner/operator.

Annual Burden Estimate: The average yearly burden for security training program development and submission, security coordinator submission, employee training documentation recordkeeping, and incident reporting is estimated to be 2,729 hours for freight railroads; 3,311 hours for PTPRs; and 6,278 hours for OTRB companies. The total average annual time burden estimate is approximately 12,318 hours. Table 5 shows the information collections and corresponding hour burdens for entities falling under the requirements of the final rule.

TABLE 5—PRA HOURS OF BURDEN

Collection	Time per response (hours)	Number of responses			3-Year time burden	Average annual time burden
		Year 1	Year 2	Year 3		
Initial Security Training Program Development and Submission						
Freight Rail	152	33	0	0	5,016	1,672
PTPR	88	47	0	0	4,136	1,379
OTRB (Large to Medium)	44	31	1	1	1,439	480
OTRB (Small)	28	174	3	3	5,062	1,687
Modified Security Training Program Development and Submission						
Freight Rail	25	30	0	0	743	248
PTPR	25	42	0	0	1,058	353
OTRB (Large to Medium)	25	28	1	1	736	245
OTRB (Small)	25	157	3	3	4,068	1,356
Security Coordinator Information Submission						
PTPR	0.5	52	6	6	32	11
OTRB	0.5	467	65	66	299	100
Employee Training Documentation Recordkeeping						
Freight Rail	0.017	136,155	4,750	4,764	2,428	809
PTPR	0.017	194,219	23,173	23,251	4,011	1,337
OTRB	0.017	39,147	5,142	5,206	825	275
Incident Reporting						
PTPR	0.05	4,652	4,652	4,652	698	233
OTRB	0.05	41,881	42,691	43,516	6,404	2,135
Total Burden (responses)	.....	.....	.....	.....	579,070	193,023
Total Burden (hours)	.....	.....	.....	.....	36,953	12,318

B. Economic Impact Analyses

1. Regulatory Impact Analysis Summary

Changes to Federal regulations must undergo several economic analyses. First, Executive Order 12866, *Regulatory Planning and Review,*[110] as supplemented by Executive Order 13563, *Improving Regulation and Regulatory Review,*[111] directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, E.O. 13771, *Reducing Regulation and Controlling Regulatory Costs,*[112] requires agencies to identify at least two regulations to be eliminated for every new regulation, and also requires that the cost of planned regulations be prudently managed and controlled through a budgeting process. Third, the Regulatory Flexibility Act of 1980[113] requires agencies to consider the economic impact of regulatory changes on small entities. Fourth, the Trade Agreement Act of 1979[114] prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fifth, UMRA requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).[115]

2. Executive Orders 12866, 13563, and 13711 Assessments

Under the requirements of Executive Orders 12866 and 13563, agencies must assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). These requirements were supplemented by Executive Order 13563, which emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. Under Executive Order 13711, *Reducing Regulation and Controlling Regulatory Costs,*[116] agencies must identify whether a

[110] 58 FR 51735 (Oct. 4, 1993).

[111] 76 FR 3821 (Jan. 21, 2011).

[112] 82 FR 9339 (Feb. 3, 2017).

[113] Public Law 96–354, 94 Stat. 1164 (Sept. 19, 1980) as codified at 5 U.S.C. 601 *et seq.*

[114] Public Law 96–39, 93 Stat. 144 (July 26, 1979), codified at 19 U.S.C. 2531–2533.

[115] *Supra* n. 63.

[116] 82 FR 9339 (Feb. 3, 2017).

rulemaking is a regulatory or deregulatory action.

In conducting these analyses, TSA has determined:

1. This rulemaking is a significant regulatory action within the meaning of Executive Order 12866 and a regulatory action under Executive Order 13771. TSA has determined that this rulemaking is not economically significant. The rule will not result in an effect on the economy of $100 million or more in any year of the analysis. The total annualized costs of the final rule over a perpetual time period using a 7 percent discount rate, in 2016 dollars, and discounted back to 2016 is $5.28 million. The rule will not adversely affect the economy, interfere with actions taken or planned by other agencies, or generally alter the budgetary impact of any entitlements.

2. TSA prepared a Final Regulatory Flexibility Analysis (FRFA), which finds that this rulemaking would likely have a regulatory cost that exceeds one percent of revenue for 47 small entities—1 freight rail and 46 OTRB owner/operators—of the total 200 small entities that would be regulated by the final rule.

3. This rulemaking would not constitute a barrier to international trade.

4. This rulemaking does not impose an unfunded mandate on State, local, or tribal governments, or on the private sector under UMRA.

In the NPRM RIA, TSA estimated that the rule would cost $157.27 million over ten years, discounted at 7 percent. In the Final RIA, TSA updated its benefit-cost analysis and estimated this regulation will cost $52.30 million over ten years, discounted at 7 percent. The change in cost estimate from the NPRM RIA to the Final RIA is due to the following:

- The final rule will require affected surface mode employees to undergo security training at least once every three years, which is a change in frequency from the annual training requirement in the NPRM. TSA updated training burden cost estimates to reflect the final rule's triennial training cycle.
- TSA updated employee population estimates in each of the three industries regulated by this final rule. In all three modes, the final rule employee population estimates decreased from the estimates in the NPRM: (1) The population of impacted freight rail employees decreased based on an updated source.[117] (2) The population of impacted PTPR employees decreased as a result of TSA using more detailed population data in this Final RIA, as well as an update in the percentage of employees performing security-sensitive roles. (3) The population of impacted OTRB employees decreased as a result of reevaluating the population of impacted OTRB owner/operators from the NPRM dataset. TSA made revisions based on new information about the owner/operator's operations (such as the lack of scheduled services), as well as the consolidation and closure of owner/operators within the industry. This re-evaluation resulted in eight fewer OTRB owner/operators than previously estimated in the NPRM, which in turn meant fewer employees were impacted.
- TSA updated its estimates of compensation rates, employee turnover rates, and various other inputs. TSA has reviewed all the inputs used in the NPRM RIA and updated them to ensure that the Final RIA uses the most recently available data.
- TSA added the cost for owner/operators to develop their own training programs in its primary cost analysis; in the NPRM RIA, only Alternative 2 made this assumption. In the primary cost analysis of the NPRM RIA, TSA assumed owner/operators would use a video provided by TSA, free of charge, to meet a majority of the training requirements. TSA still plans to make this video available, however for the purpose of presenting the full range of possible costs for owner/operators from the final rule, TSA decided to include the cost of developing a custom training program in the Final RIA. Because of this change, TSA increased the time burden for owner/operators to develop a training program. TSA also increased the time burden for TSA to review, modify, and re-review these programs. Lastly, TSA increased its estimate of hours spent per inspection because TSA believes Transportation Security Inspectors will need more time to inspect owner/operators on the particulars of their unique training program.
- TSA revised its assumption that owner/operators will, on average, update their training program every five years (as assumed in the NPRM RIA) to every three years. TSA made this change because it better aligns with the new assumption that owner/operators would create their own training program. TSA assumes a custom training program would involve more owner/operator-specific circumstantial changes and those would occur, on average, more often. This change increased the estimated cost to owner/operators and TSA because they will, respectively, submit and review training programs more frequently within a ten-year period.
- TSA added the cost for a name check of new security coordinators against its Terrorist Screening Database. This cost is absorbed by TSA, not owner/operators nor the security coordinators.
- TSA revised its time burden estimate for recordkeeping from 15 seconds to 1 minute. This more closely aligns to previous estimates TSA has made for other employee-specific recordkeeping requirements.

Table 6 shows the cost components that TSA expects industry and Government will incur from implementing the final rule. This table compares these cost components to their respective estimates in the NPRM and describes the changes made from the original analysis.

[117] The Final RIA used the 2017 version of ''AAR Railroad Facts'' versus the 2014 version used in the NPRM.

TABLE 6—10-YEAR TOTAL COST OF NPRM VS FINAL RULE

[Discounted at 7 percent, in $ thousands]

Requirements	Section	NPRM and FR comparison			Description	Significant change from NPRM to final rule
		NPRM	Final rule	Difference		
Training Cost	1580.113, 1582.113, and 1584.113.	$152,277	$43,429	($108,848)	Requirement to train security-sensitive employees on required elements (one of the elements is expanded for freight rail) of security training.	Changed cost estimate to reflect three-year training cycle. Updated and refined population data of security-sensitive employees. Overall estimate of affected employees decreased from the NPRM.
Training Plan	1570.109	1,653	4,372	2,718	Requirement to submit a training program to TSA. Costs include planning, drafting, review and submission.	Added the cost for creating custom training plans; TSA previously, assumed they would use the TSA-provided video.
Security Coordinator.	1570.201	77	48	(29)	Requirement to assign a security coordinator and an alternate to serve as a security liaison with TSA. Costs include initial and updated submissions from security coordinator turnover.	Added the TSA cost to perform a name check of new security coordinators against the Terrorist Screening Database.
Incident Reporting.	1570.203	2,052	2,404	353	Requirement to report significant security concerns within 24 hours of initial discovery. TSA assumes incident reporting will occur telephonically.	Included additional post-call administrative costs for TSA.
Recordkeeping ...	1570.121	592	875	283	Requirement to maintain security training records for each individual trained. These records may be stored either electronically or printed on paper and filed.	(1) Decreased cost associated with number of records due to reduced frequency of training and (2) increased the time burden per record from 15 seconds to 1 minute. This estimate is also more aligned with previous estimates TSA made for recordkeeping of other vetting programs.
Inspections	1570.9	622	1,175	553	Availability for inspection by TSA for compliance with the final rule. Costs assume annual inspections for each owner/operator; industry cost to prepare for and host TSA inspections. and presentation of training records and program curriculum when requested by TSA during inspection.	No significant changes. Cost difference due to updates in wages and population estimates.
Total Costs ..	.....	157,274	52,303	(104,971)		

TSA has prepared an analysis of its estimated costs and benefits, summarized in the following paragraphs. The OMB Circular A–4 Accounting Statement for this final rule is in section VIII.B.3. When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. For this rule's period of analysis, TSA uses a 10-year period of analysis to estimate the initial and recurring costs of the regulated surface mode owner/operators and new owner/operators that are expected due to industry growth.

TSA concluded the following about the current, or baseline, training

environment for freight rail, public transportation and passenger railroad (PTPR), and OTRB employees (*see* section 1.8 of the RIA placed in the docket for further detailed information on the current baseline):

There are 574 U.S. freight rail owners/operators and are composed of 7 Class I, 21 Class II, and 546 Class III railroads.[118] A total of 33 (7 Class I, 8 Class II, and 18 Class III) out of the 574 U.S. freight rail owner/operators carry RSSM through an HTUA and would be affected by the final rule.[119] These 33 freight rail owner/operators provide security awareness [120] and chain of custody and control [121] trainings to their employees. These trainings address two of the required elements of security training required by the final rule in § 1580.115 (Security training and knowledge for security-sensitive employees: Prepare and Assess). Additionally, freight rail owner/operators are already required to comply with the requirements to assign security coordinators and report significant security concerns to TSA under current 49 CFR 1580. Table 7 below identifies the requirements of the final rule implemented by freight rail owner/operators. The check marked items in the table represent existing requirements under PHMSA's regulations (*see* 49 CFR 172.704 and 1580.107) and, therefore, do not represent additional burden to the freight rail owners/operators.

Table 7—Freight Rail Owner/Operator Baseline Assessment

Proposed Population	Training Components					Security Coordinators	Report Significant Security Concerns
	Prepare	Chain of Custody	Observe	Assess	Respond		
Freight rail		✓		✓		✓	✓

Note: Check marked items represents existing requirements. The "prepare" element of the training curriculum under proposed part 1580 includes training on the chain of custody requirements that are in current part 1580. For purposes of this table, "Prepare" refers to everything but "chain of custody," and "Chain of custody" only refers to that topic.

There are nearly 6,800 public transportation organizations in the United States.[122] Of these, 47 PTPR owner/operators [123] fall within the applicability of the final rule. Twenty-four of these 47 PTPR owner/operators effectively provide training to their employees on security awareness and employee- and company-specific security programs and measures.[124] This training address two of the required elements of security training required by the final rule in § 1582.115 (Prepare and Assess). Additionally, 24 PTPR owner/operators with rail operations are already required to comply with the requirements to assign security coordinators and report significant security concerns to TSA under current 49 CFR part 1580. Table 8 below identifies the requirements of the final rule already implemented by PTPR owner/operators. The check marked items in the table represent existing requirements under 49 CFR part 1580 and, therefore do not represent additional burden to the freight rail owners/operators.

[118] AAR, ''Railroad Facts, 2017 Edition,'' at pg.3 (2017).

[119] TSA used its railcar tracking system that monitors toxic inhalant hazard cars, the Rail Asset Integrated Logistics System, (RAILS), to identify freight rail owner/operators that transported one or more shipments of RSSM during the period in calendar year 2017.

[120] As required by PHMSA. *See* 49 CFR 172.704.

[121] In place because of the chain of custody requirement in 49 CFR 1580.107.

[122] APTA, ''2016 Public Transportation Fact Book'' (Feb. 2017), available at *http://www.apta.com/resources/statistics/Documents/FactBook/2016-APTA-Fact-Book.pdf.*

[123] TSA elicited and used input from SMEs in its Surface Division, combined with data from the Federal Transit Administration's (FTA) National Transit Database (NTD) to identify the 47 PTPR owner/operators.

[124] Agencies identified using latest evaluation from TSA's BASE assessment. Information on BASE assessment can be found at: *https://www.tsa.gov/news/top-stories/2015/09/21/transit-agencies-earn-high-ratings-through-base-program.*

Table 8—PTPR Owner/Operators Baseline Assessment

Proposed Population	Training Components				Security Coordinators	Report Significant Security Concerns
	Prepare	Observe	Assess	Respond		
PTPR owners/operators with rail service and a robust training program	✓		✓		✓	✓
PTPR owners/operators with rail service and no robust training program					✓	✓
Bus-only PTPR owners/operators with a robust training program	✓		✓			
Bus-only PTPR owners/operators with no robust training program						

Note: Check marked items represents existing requirements.

There are 2,990 U.S. companies in the motorcoach industry.[125] Of these, 205 [126] fall within the applicability of the final rule. Three of the 205 are large OTRB companies that currently use the TSA-supplied First Observer™ program, which covers a majority of the 9/11 Act security training requirements, to train their employees. This training addresses three of the security training elements of this final rule (Observe, Assess, and Respond). Table 9 identifies the requirements of this final rule implemented by OTRB owner/operators. The check marked items in the table represent the training components already covered by the First Observer™ program and, therefore do not represent additional burden to the OTRB owners/operators currently using this program compared to the ''no-action'' baseline.[127] In Appendix A of the RIA, however, TSA has also monetized the cost of their current participation in First Observer™. TSA estimated this cost at $0.57 million to these owner/operators over 10 years (discounted at 7 percent).[128]

Table 9—OTRB Owner/Operators Baseline Assessment

Proposed Population	Training Components				Security Coordinators	Report Significant Security Concerns
	Prepare	Observe	Assess	Respond		
Three "large" OTRB owners/operators		✓	✓	✓		
Remaining OTRB owner/operators						

Note: Check marked items represents voluntary participation in First Observer™.

TSA summarizes the costs of the final rule to be borne by four affected parties: freight railroad owner/operators, PTPR owner/operators, OTRB owner/operators, and TSA. As displayed in Table 10, TSA estimates the 10-year total cost of this final rule to be $73.17 million undiscounted, $62.82 million discounted at 3 percent, and $52.30 million discounted at 7 percent. The costs to industry (all three surface modes) comprise approximately 96.2 percent of the total costs of the rule; and the remaining costs are incurred by TSA.

TABLE 10—TOTAL COST OF THE FINAL RULE BY ENTITY

[$ millions]

Year	Freight rail	PTPR	OTRB	TSA	Total final rule cost		
					Undiscounted	Discounted at 3%	Discounted at 7%
1	$8.82	$5.74	$2.28	$0.63	$17.46	$16.95	$16.32
2	0.31	0.67	0.42	0.21	1.60	1.50	1.39
3	0.31	0.67	0.42	0.21	1.61	1.47	1.31

[125] American Bus Association Foundation, ''Motorcoach Census 2015'' (Oct. 9, 2017), available at *https://www.buses.org/assets/images/uploads/pdf/Motorcoach_Census_2015.pdf.*

[126] TSA relied on a variety of sources to identify the 205 owner/operators: Intercity Bus Security Grant Program (IBSGP) applications submitted to FEMA and reviewed by TSA, the American Intercity Bus Riders Association (AIBRA) intercity bus service operator list, consultations with ABA, and internet research of websites like *GotoBus.com* and other publicly available sources of information.

[127] OMB, ''Circular A–4,'' at 2, available at *https://www.whitehouse.gov/sites/default/files/omb/assets/regulatory_matters_pdf/a-4.pdf.* (''Benefits and costs are defined in comparison with a clearly stated alternative. This normally will be a 'no action' baseline: What the world will be like if the proposed rule is not adopted.'')

[128] OMB also requires TSA to consider a ''pre-statute'' baseline. Id. at 16. Costs of First Observer™ have accrued since passage of the 9/11 Act and are part of this ''pre-statute'' baseline.

TABLE 10—TOTAL COST OF THE FINAL RULE BY ENTITY—Continued
[$ millions]

Year	Freight rail	PTPR	OTRB	TSA	Total final rule cost		
					Undiscounted	Discounted at 3%	Discounted at 7%
4	8.08	4.49	2.02	0.27	14.87	13.21	11.34
5	0.58	1.10	0.56	0.22	2.46	2.12	1.75
6	0.58	1.11	0.57	0.22	2.48	2.07	1.65
7	7.64	3.82	1.91	0.28	13.65	11.10	8.50
8	0.82	1.41	0.68	0.23	3.14	2.48	1.83
9	0.83	1.42	0.69	0.23	3.17	2.43	1.72
10	7.25	3.35	1.85	0.29	12.74	9.48	6.48
Total	35.21	23.78	11.40	2.78	73.17	62.82	52.30
Annualized	.....	.....	.....	.....	.....	7.36	7.45

Note: Totals may not add due to rounding.

TSA estimates the 10-year costs to the freight railroad industry to be $35.21 million undiscounted, $30.18 million discounted at 3 percent, and $25.09 million discounted at 7 percent, as displayed by cost categories in Table 11.

Table 11—Total Cost to the Freight Rail Industry from the Final Rule ($ millions)

Year	Training Costs	Training Plan Costs	Recordkeeping Costs	Inspection Costs	Total Freight Rail Cost		
					Undiscounted	Discounted at 3%	Discounted at 7%
1.....	$8.26	$0.40	$0.15	$0.00	$8.82	$8.56	$8.24
2.....	0.29	0.00	0.01	0.01	0.31	0.29	0.27
3.....	0.29	0.00	0.01	0.01	0.31	0.28	0.25
4.....	7.79	0.14	0.14	0.01	8.08	7.18	6.17
5.....	0.55	0.00	0.01	0.01	0.58	0.50	0.41
6.....	0.55	0.00	0.01	0.01	0.58	0.48	0.39
7.....	7.35	0.14	0.14	0.01	7.64	6.21	4.76
8.....	0.79	0.00	0.01	0.01	0.82	0.65	0.48
9.....	0.80	0.00	0.01	0.01	0.83	0.63	0.45
10....	6.97	0.14	0.13	0.01	7.25	5.39	3.68
Total					$35.21	$30.18	$25.09
Annualized						$3.54	$3.57

Note: Totals may not add due to rounding.

TSA estimates the 10-year costs to the PTPR industry to be $23.78 million undiscounted, $20.48 million discounted at 3 percent, and $17.12 million discounted at 7 percent, as displayed by cost categories in Table 12.

Table 12—Total Cost to the PTPR Industry from the Final Rule ($ millions)

Year	Training Costs	Training Plan Costs	Security Coordinator Costs	Incident Reporting Costs	Recordkeeping Costs	Inspection Costs	Total PTPR Cost		
							Undiscounted	Discounted at 3%	Discounted at 7%
1…..	$5.13	$0.46	$0.00	$0.02	$0.12	$0.00	$5.74	$5.57	$5.36
2…..	0.61	0.00	$0.00	0.02	$0.01	0.02	0.67	0.63	0.58
3…..	0.61	0.00	$0.00	0.02	$0.01	0.02	0.67	0.61	0.54
4…..	4.16	0.20	$0.00	0.02	$0.10	0.02	4.49	3.99	3.43
5…..	1.04	0.00	$0.00	0.02	$0.02	0.02	1.10	0.95	0.79
6…..	1.04	0.00	$0.00	0.02	$0.02	0.02	1.11	0.93	0.74
7…..	3.50	0.20	$0.00	0.02	$0.08	0.02	3.82	3.10	2.38
8…..	1.34	0.00	$0.00	0.02	$0.03	0.02	1.41	1.12	0.82
9…..	1.35	0.00	$0.00	0.02	$0.03	0.02	1.42	1.09	0.77
10…	3.04	0.20	$0.00	0.02	$0.07	0.02	3.35	2.50	1.70
Total							$23.78	$20.48	$17.12
Annualized								$2.40	$2.44

Note: Totals may not add due to rounding.

TSA estimates the 10-year costs to the OTRB industry to be $11.40 million undiscounted, $9.74 million discounted at 3 percent, and $8.06 million discounted at 7 percent, as displayed by cost categories in Table 13.

Table 13—Total Cost to the OTRB Industry from the Final Rule ($ millions)

Year	Training Costs	Training Plan Costs	Security Coordinator Costs	Incident Reporting Costs	Recordkeeping Costs	Inspection Costs	Total OTRB Cost		
							Undiscounted	Discounted at 3%	Discounted at 7%
1…..	1.20	0.88	0.02	0.16	0.02	0.00	2.28	2.21	2.13
2…..	0.16	0.02	0.00	0.16	0.00	0.07	0.42	0.39	0.36
3…..	0.16	0.02	0.00	0.17	0.00	0.07	0.42	0.39	0.34
4…..	0.98	0.78	0.00	0.17	0.01	0.07	2.02	1.80	1.54
5…..	0.27	0.03	0.00	0.17	0.00	0.08	0.56	0.48	0.40
6…..	0.27	0.03	0.00	0.18	0.00	0.08	0.57	0.48	0.38
7…..	0.84	0.80	0.00	0.18	0.01	0.08	1.91	1.55	1.19
8…..	0.36	0.05	0.00	0.18	0.01	0.08	0.68	0.53	0.39
9…..	0.36	0.05	0.00	0.19	0.01	0.08	0.69	0.53	0.37
10…	0.75	0.81	0.00	0.19	0.01	0.08	1.85	1.38	0.94
Total							$11.40	$9.74	$8.06
Annualized								$1.14	$1.15

Note: Totals may not add due to rounding.

TSA estimates the 10-year costs to TSA to be $2.78 million undiscounted, $2.41 million discounted at 3 percent, and $2.03 million discounted at 7 percent, as displayed by cost categories in Table 14.

Table 14—Total Cost to TSA from the Final Rule ($ millions)

Year	Training Plans	Security Coordinators	Incident Reporting	Inspection	Total TSA Costs		
					Undiscounted	Discounted at 3%	Discounted at 7%
1.....	$0.36	$0.01	$0.14	$0.13	$0.63	$0.61	$0.59
2.....	0.00	0.00	0.14	0.06	0.21	0.19	0.18
3.....	0.00	0.00	0.14	0.06	0.21	0.19	0.17
4.....	0.06	0.00	0.15	0.06	0.27	0.24	0.21
5.....	0.00	0.00	0.15	0.06	0.22	0.19	0.15
6.....	0.00	0.00	0.15	$.06	0.22	0.18	0.15
7.....	0.06	0.00	0.15	0.06	0.28	0.23	0.17
8.....	0.01	0.00	0.16	0.07	0.23	0.18	0.13
9.....	0.01	0.00	0.16	0.07	0.23	0.18	0.13
10.....	0.06	0.00	0.16	0.07	0.29	0.22	0.15
Total					$2.78	$2.41	$2.03
Annualized						$0.28	$0.29

Note: Totals may not add due to rounding.

This final rule will enhance surface transportation security by reducing the risk of terrorist attacks in four ways. First, the rule ensures employees on the frontline of higher-risk surface transportation systems and operations (defined as ''security-sensitive employees'') are trained on how to observe, assess, and respond to a security threat, enhancing their capabilities to take appropriate actions and mitigate the consequences of any threat or incident. Second, security-sensitive employees with responsibilities under their employer's security plan or for specific security measures will be prepared through training to perform any actions associated with that responsibility. Third, there will be more effective communication between TSA and all higher-risk operations through the designation of security coordinators by all higher-risk operations. Finally, the expanded scope of owner/operators required to report significant security concerns will enhance TSA's ability to identify risks and recommend appropriate actions based on a more comprehensive picture of threats to surface transportation security.

While training and the other requirements of this final rule are not absolute deterrents for terrorists intent on carrying out attacks on surface modes of transportation, TSA expects the probability of success for such attacks to decrease when the requirements of this rule are fully implemented.

TSA uses a break-even analysis to frame the relationship between the potential benefits of the final rule and the costs of implementing the rule. When it is not possible to quantify or monetize a majority of the incremental benefits of a regulation, OMB recommends conducting a threshold, or ''break-even'' analysis. According to OMB Circular No. A–4, ''Regulatory Analysis,'' such an analysis answers the question ''How small could the value of the non-qualified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?'' [129]

To conduct the break-even analysis, TSA evaluates three composite scenarios for each the three modes covered by the final rule. For each scenario, TSA calculates a total monetary consequence from an estimated statistical value of the human casualties and capital replacement resulting from the attack (see Section 4.3 of the Final RIA for a more detailed description of these calculations; however, many assumptions regarding specific terrorist attacks scenarios are SSI and cannot be publicly released).

Table 15 presents the composite or weighted average of direct consequences from a successful attack on each mode.

[129] *See id.*

[130] As explained in the Final RIA, available in the docket, to monetize injuries, TSA used two approaches (depending on whether the injury was due to exposure to hazardous chemicals). To monetize ''non-chemical'' injuries, TSA uses guidance from the Department of Transportation for valuing injuries based on the Abbreviated Injury Scale. To monetize chemical-related injuries, TSA obtained information on the cost of medical treatment for poisoning injuries.

[131] Total Direct Consequences = (Deaths × $9.6 million VSL) + (Severe injuries × $2.55 million) + (Moderate injuries × $0.45 million) + (Severe chemical injuries × $43,743) + (Moderate chemical injuries × $1,687) + Public property loss + Private property loss + Rescue and clean-up cost.

Table 15—Composite Monetized Consequences from a Successful Attack[130]

Variables		Transportation Mode		
		Freight	PTPR	OTRBs
Weighted Average Values	Number of Deaths	29.41	36.22	38.34
	Number of Severe Injuries (non-chemical)	39.77	43.69	0.70
	Number of Moderate Injuries (non-chemical)	34.07	49.60	0.45
	Number of Chemical Severe Injuries	42.30	0.00	0.00
	Number of Chemical Moderate Injuries	80.21	0.00	0.00
	Monetized Public Infrastructure Loss ($ thousands)	$11,406	$5,322	$48
	Monetized Private Property Loss ($ thousands)	$18,429	$95	$424
	Monetized Rescue and Cleanup ($ thousands)	$74,806	$704	$435
Total Monetized Direct Consequences[131] ($ thousands)		$505,866	$487,799	$370,997

Note: Totals may not add due to rounding.

TSA compared the estimated direct monetary costs of an attack to the annualized cost (discounted at 7 percent) to industry and TSA from the final rule for each mode to estimate how often an attack of that nature would need to be averted for the expected benefits to equal estimated costs. Table 16 presents the results of the break-even analysis for each mode. For example, Table 16 shows that if the freight rail training requirements in this rule prevents one freight rail terrorist attack every 141 years, this rule ''breaks-even'' (the benefits equal the costs).

The break-even analysis does not include the difficult-to-quantify indirect costs of an attack or the macroeconomic impacts that could occur due to a major attack. In addition to the direct impacts of a terrorist attack in terms of lost life and property, there are other more indirect impacts that are difficult to measure. As noted by Cass Sunstein in *Laws of Fear,* ''. . . fear is a real social cost, and it is likely to lead to other social costs.'' [132] In addition, Ackerman and Heinzerling state ''. . . terrorism 'works' through the fear and demoralization caused by uncontrollable uncertainty.'' [133] As devastating as the direct impacts of a successful terrorist attack can be in terms of the immediate loss of life and property, avoiding the impacts of the more difficult to measure indirect effects are also substantial benefits of preventing a terrorist attack.

TABLE 16—BREAK-EVEN ANALYSIS RESULTS

[$ millions]

Modes	Weighted average direct costs of a successful attack a	Annualized cost of the final rule at 7% b	Breakeven averted attack frequency c = a ÷ b
Freight Rail	$505.87	$3.60	One attack every 141 years.
PTPR	487.80	2.48	One attack every 197 years.
OTRB	371.00	1.37	One attack every 271 years.

Note: Totals may not add due to rounding.

3. OMB A–4 Statement

The OMB A–4 Accounting Statement (in Table 17) presents annualized costs and qualitative benefits of the final rule.

[132] Cass R. Sunstein, *Laws of Fear* at 127 (2005).

[133] Frank Ackerman and Lisa Heinzerling, *Priceless On Knowing the Price of Everything and the Value of Nothing* at 136 (2004).

TABLE 17—OMB A–4 ACCOUNTING STATEMENT

[in $ millions, 2017 dollars]

Category	Primary estimate		Minimum estimate	Maximum estimate	Source citation (Final RIA, preamble, etc.)
Benefits ($ millions)					
Annualized monetized benefits (discount rate in parentheses).	N/A	N/A	N/A	N/A	Final RIA
Unquantified benefits	The requirements proposed in this rule produce benefits by reducing security risks through training security-sensitive surface mode employees to identify and/or mitigate an attempted terrorist attack.				Final RIA
Costs ($ millions)					
Annualized monetized costs (discount rate in parentheses).	(7%) (3%)	$7.45 $7.36	.....	.....	Final RIA
Annualized quantified, but unmonetized, costs.	0		0	0	Final RIA
Qualitative costs (unquantified)	N/A				Final RIA
Transfers					
Annualized monetized transfers: "on budget".	N/A		N/A	N/A	Final RIA
From whom to whom?	N/A		N/A	N/A	None
Annualized monetized transfers: "off-budget".	N/A		N/A	N/A	Final RIA
From whom to whom?	N/A		N/A	N/A	None
Miscellaneous analyses/category	Effects				Source citation (NPRM RIA, preamble, etc.)
Effects on State, local, and/or tribal governments.	None				Final RIA
Effects on small businesses	Prepared FRFA				FRFA (Chapter 6 RIA)
Effects on wages	None				None
Effects on growth	None				None

4. Alternatives Considered

In addition to the final rule, TSA also considered two alternative policies. In comparison to the final rule, the first alternative (Alternative 1) removes requirements for recordkeeping, security incident reporting, and security coordinators for bus-only PTPR owner/operators. This alternative also removes the requirement to train freight railroad security-sensitive employees on chain of custody and control requirements.[134] The second alternative (Alternative 2) increases the training frequency to an annual basis and expands the population of owners/operators to all who operate within any UASI, which includes the entire metropolitan statistical area.[135] All other requirements remain the same.

Though not the least costly option, TSA selects the requirements in this final rule as the preferred alternative. TSA rejected Alternative 1 because it omitted the following important security measures TSA proposed in the NPRM: (1) Recordkeeping requirements to ensure TSA can determine compliance (all modes), (2) expanding security coordinator requirements to provide a security point of contact for bus-only operations (PTPR), (3) expanding reporting requirements for security incidents to ensure TSA has a more complete picture of potential threats to surface transportation (PTPR and OTRB); and (4) ensuring freight railroad security-sensitive employees with responsibilities under TSA's chain of custody and control requirements have the necessary training to ensure compliance with these security measures in place since promulgation of TSA's Rail Security Rule.[136] By including these security measures, TSA can ensure compliance with the rule, obtain a complete picture of potential threats to surface transportation across multiple modes, and enhance compliance with security measures required for freight railroads.

TSA also rejected Alternative 2. As discussed in the NPRM, TSA applied a risk-based approach to determining applicability of this final rule.[137] Expanding the population would be inconsistent with TSA's commitment to risk-based security.[138] TSA is also rejecting requiring annual recurrent training in response to comments

[134] Table 64 in the RIA found in the docket provides a section-by section analysis of which regulatory provisions are statutorily required and which provisions are discretionary.

[135] As previously noted, *see* section VII.C.4. of the preamble to this final rule, TSA proposed an annual recurrent training requirement in the NPRM. *See also* 81 FR at 91348. For the NPRM, TSA also considered an alternative to "train security-sensitive employees once every three years using TSA-provided materials. *Id.* at 91379. In response to comments, TSA is adopting a three-year recurrent training cycle for purposes of the final rule, making the annual recurrent training requirement the alternative considered for purposes of the alternatives analysis.

[136] 73 FR 72129, 72130–72179 (Nov. 26, 2008). "Rail Transportation Security; Final Rule."

[137] *See supra* n. 13.

[138] *Id.*.

received on the NPRM.[139] In response to these comments which suggested longer time periods between training, TSA modified the recurrent training requirement to at least once every three years in the final rule, and rejected the annual recurrent training requirement in Alternative 2.

TABLE 18—COMPARISON OF COSTS BETWEEN ALTERNATIVES

[in millions]

	Initial Affected population (number of owner/operators)	Requirements	10-Year costs (in $ millions) at a 7% discount rate		
			Industry	TSA	Total
Final Rule	33 Freight Rails 47 PTPRs 205 OTRBs	1. Provide security training to security-sensitive employees once every three years. 2. Designate a security coordinator (expanded requirement to include bus-only PTPR and OTRB). 3. Report significant security incidents to TSA (expanded requirement to include bus-only PTPR and OTRB) Maintain employee training records and. 4. Provide access to TSA and proof of compliance.	$50.28	$2.03	$52.30
Alternative 1		1. Provide security training to security-sensitive employees once every three years (except for Chain of custody and control);. 2. Designate a security coordinator (expanded requirement limited to OTRB). 3. Maintain employee training records and. 4. Provide access to TSA and proof of compliance.	48.03	0.99	49.02
Alternative 2	69 Freight Rails 253 PTPRs 403 OTRBs	1. Provide annual security training to security-sensitive employees within expanded applicability. 2. Designate a security coordinator. 3. Report significant security incidents to TSA. 4. Maintain employee training records and. 5. Provide access to TSA and proof of compliance.	219.54	4.52	224.05

Note: Totals may not add due to rounding.

5. Regulatory Flexibility Assessment

The RFA [140] requires agencies to consider the impacts of their rules on small entities. TSA performed a Final Regulatory Flexibility Analysis (FRFA) to analyze the impact to small entities affected by the final rule.[141] The RFA analysis presented below is a summary of the FRFA, including the six elements in 5 U.S.C. 604.

a. A Statement of the Need for, and Objectives of, the Rule. Sections 1408, 1517, and 1534 of the 9/11 Act require TSA to issue a security training rule requiring owner/operators of various modes of surface transportation to provide training to frontline employees of freight rail, PTPR, and OTRB employees. Owner/operators are required to submit a training program to TSA for review that will be marked SSI. An owner/operator must also keep records of whether each employee has successfully completed their training. Additionally, TSA will collect security coordinator and alternate coordinator information from entities covered in the final rule, as well as require reporting of suspicious activities or incidents by these owner/operators. TSA requests this information from owner/operators to be better prepared to respond to emergencies or incidents and to have designated points of contacts with covered entities when information needs to be shared or retrieved. TSA requests reporting of security-related incidents and suspicious activities to assess if there is a new threat or increased threat to the surface modes of transportation.

b. A Statement of the Significant Issues Raised by Public Comments in Response to the IRFA, a Statement of the Assessment of the Agency of Such Issues, and a Statement of Any Changes Made in the Proposed Rule as a Result of Such Comments. The public did not submit significant comments during the comment period specifically on the IRFA. However, elsewhere in in the preamble of the final rule, TSA answered public comments on the cost estimate of the rule.

c. Description of and an Estimate of the Number of Small Entities to Which the Rule Will Apply or an Explanation of Why No Such Estimate is Available. Under the RFA, the term ''small entities'' comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and small governmental jurisdictions with populations of less than 50,000. Individuals and States are not considered ''small entities'' based on the definitions in the RFA (5 U.S.C. 601).

The PTPR owner/operators affected by this final rule are not considered small entities because they are either owned/operated by governmental jurisdictions that exceed the RFA population threshold of 50,000 or a

[139] *See* section VI.C.4 of this final rule.

[140] *See supra* n. 113.

[141] *See* Chapter 6 of the Final RIA in the docket for the full FRFA.

business that exceeds the Small Business Administration's (SBA) size threshold. Only freight rail and OTRB owner/operators have small entities affected by the final rule.

The final rule requires security training for Class I freight rail owner/operators and freight rail owner/operators that transport RSSM in one or more HTUAs [142] or host high-risk passenger rail operations on their tracks. TSA identified 33 freight railroad entities affected by the final rule.

TSA uses the SBA size standards to identify that 18 of the 33 freight rail owner/operators affected by the final rule are considered a small business. TSA calculates that final rule's requirements are estimated to cost $61.82 per employee and $18,390.32 per freight rail owner/operator. Of these 18 small freight rail owner/operators, TSA estimates that one of these freight rail owner/operators would likely have a regulatory cost that exceeds one percent of their revenue. Table 19 presents the likely distribution of costs for small freight rail owner/operators.

TABLE 19—COSTS AS A PERCENT OF REVENUE FOR SMALL FREIGHT RAIL OWNER/OPERATORS

Revenue impact range	Number of entities	Percent of entities
0% < Impact ≤ 1%	17	94
1% < Impact ≤ 3%	0	0
3% < Impact ≤ 5%	1	6
5% < Impact ≤ 10%	0	0
Above 10%	0	0
Total	18	100.0

TSA identified 205 OTRB owner/operators entities affected by the final rule. Using SBA's size threshold, TSA estimates that 182 OTRB owner/operators regulated by the final rule are considered a small business. TSA calculates that the final rule's requirements are estimated to cost $35.68 per employee and $5,759.94 per entity to these OTRB owner/operators. Using a relevant sample of these 143 small OTRB owner/operators, TSA estimates that 32% of them would likely have a regulatory cost that exceeds one percent of their revenue. Table 20 presents the likely distribution of costs for this sample of small OTRB owner/operators.

TABLE 20—COSTS AS A PERCENT OF REVENUE FOR SMALL OTRB OWNER/OPERATORS

Revenue impact range	Number of entities	Percent of entities
0% < Impact ≤ 1%	97	68
1% < Impact ≤ 3%	36	25
3% < Impact ≤ 5%	6	4
5% < Impact ≤ 10%	4	3
Above 10%	0	0
Total	143	100.0

d. The Response of the Agency to Any Comments Filed by the Chief Counsel for Advocacy of the Small Business Administration in Response to the Proposed Rule, and a Detailed Statement of Any Change Made to the Proposed Rule in the Final Rule as a Result of the Comments. The Small Business Administration did not submit any comments during the comment period for the NPRM.

e. A Description of the Projected Reporting, Recordkeeping, and Other Compliance Requirements of the Final Rule, Including an Estimate of the Classes of Small Entities that Will Be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record. This final rule's reporting, recordkeeping and other compliance requirements will include submission of security training programs, security coordinator and security incident information, retention of training records, and availability for compliance inspections. TSA assumes that any training program, incident report, security coordinator package, or other information submitted to TSA will be completed by management-level personnel. TSA also assumes that owner/operators will have a manager prepare before a TSA compliance inspection. TSA assumes the recordkeeping requirements of the final rule will be fulfilled by employees with administrative and clerical skills.

f. A Description of the Steps the Agency has Taken to Minimize Significant Economic Impact on Small Entities Consistent with the Stated Objectives of Applicable Statutes, including a Statement of the Factual, Policy, and Legal Reasons for Selecting the Alternative Adopted in the Final Rule and Why Each of the Other Significant Alternatives to the Rule Considered by the Agency which Affect the Impact on Small Entities was Rejected. TSA will allow owner/operators to develop their own training programs (which must receive TSA approval). TSA will give owner/operators the flexibility to use different training materials to satisfy the final rule's training requirements. Additionally, in an effort to create a baseline for security training and minimize costs on regulated owner/operators, TSA will provide training videos to incorporate the non-entity-specific training requirements laid out in the final rule. TSA will make these training videos available to all owner/operators, including small entities not

[142] *See* Appendix A to part 1580 of this final rule for list of HTUAs.

covered by the high-risk criteria, which could be used on a voluntary basis by entities seeking to improve their security posture.

TSA considered two other feasible alternatives, detailed in chapter 5 of the Final RIA, in addition to the final rule.

Alternative 1: Requirements Limited to Those Expressly Authorized by Statute. In comparison to the final rule, the first regulatory alternative TSA considered would limit the requirements to those expressly authorized by the 9/11 Act or other relevant statutory provisions, such as 49 U.S.C. 114. Under this alternative, the applicability of owner/operators required to comply and employees to be trained would remain the same and the recurrence of training would be the same as the final rule (once every three years), but TSA would remove the following requirements:

- Recordkeeping (final rule requires retention of records necessary to validate compliance);
- Training freight rail employees on the chain of custody procedures required by TSA's regulations (*see* § 1580.205 for chain of custody and control requirements relocated from § 1580.107);
- Security coordinators and reporting security incidents by bus-only PTPR owner/operators; and
- Reporting security incidents by OTRB owner/operators.

The alternative would still include requirements to provide security training to security-sensitive employees (with the exception of chain of custody and control) once every three years, designating security coordinators for OTRB owner/operators, and providing access to TSA to inspect for compliance. The narrower scope from this alternative means the costs to small businesses would be less than the final rule. TSA rejected this alternative based on the determination that recordkeeping is implicitly required as it is a necessary component of enforcing a regulation, and the other measures are necessary for consistent application of the TSA's requirements imposed to enhance surface transportation security.

Alternative 2: Increased Population Alternative with Program Creation Assumptions. TSA considered a second regulatory alternative that would require annual training and increase the population of owner/operators required to comply with the final rule. For Alternative 2, TSA considered expanding the scope of applicability to any freight railroad, PTPR system, or OTRB operator operating fixed-route service to, through, or from a UASI. Under this alternative, TSA would impose additional burdens to a significant number of small owner/operators, including those that TSA has not determined to be higher-risk. This alternative could have a disproportionate impact upon small entities. Alternative 2 would increase total costs upon the regulated community as a whole. Additionally, TSA received comments to the NPRM (section VI.C.4 of this preamble) that suggested longer time periods between training, such as two or three years. In response to these comments, TSA modified the recurrent training requirement to at least once every three years in the final rule, and rejected the annual recurrent training requirement in Alternative 2. TSA rejected this alternative as it is inconsistent with the agency's risk-based security policy determination to focus on higher-risk owner/operators and commitment to outcomes-based regulations. TSA also rejected this alternative because of its annual recurrent training requirement.

6. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this final rule and has determined that it would have only a domestic impact and therefore no effect on any trade-sensitive activity.

7. Unfunded Mandates Assessment

The Unfunded Mandates Reform Act of 1995 is intended, among other things, to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of UMRA requires each Federal agency to prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may result in a $100 million or more expenditure (adjusted annually for inflation) in any one year by State, local, and tribal governments, in the aggregate, or by the private sector; such a mandate is deemed to be a ''significant regulatory action.'' [143]

This final rule does not contain such a mandate. Therefore, the requirements in Title II of UMRA do not apply and TSA has not prepared a statement.

C. Executive Order 13132, Federalism

TSA has analyzed this rulemaking under the principles and criteria of Executive Order 13132, Federalism. We determined that this action would not have a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government, and therefore would not have federalism implications.

D. Environmental Analysis

TSA has reviewed this rulemaking for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4347) and has determined that this action will not have a significant effect on the human environment. This action is covered by categorical exclusion (CATEX) number A3(b) in DHS Management Directive 023–01 (formerly Management Directive 5100.1), Environmental Planning Program, which guides TSA compliance with NEPA.

E. Energy Impact Analysis

The energy impact of this rulemaking has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Public Law 94–163, as amended (42 U.S.C. 6362). TSA has determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects

49 CFR Part 1500

Air carriers, Air transportation, Aircraft, Airports, Bus transit systems, Commuter bus systems, Law enforcement officer, Maritime carriers, Over-the-Road buses, Public transportation, Rail hazardous materials receivers, Rail hazardous materials shippers, Rail transit systems, Railroad carriers, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures, Transportation facility, Vessels.

49 CFR Part 1520

Air carriers, Air transportation, Aircraft, Airports, Bus transit systems, Commuter bus systems, Law enforcement officer, Maritime carriers, Over-the-Road buses, Public transportation, Rail hazardous materials receivers, Rail hazardous materials shippers, Rail transit systems, Railroad carriers, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures, Transportation facility, Vessels.

[143] *Supra* n. 63 as codified at 2 U.S.C. 1532.

49 CFR Part 1570

Commuter bus systems, Crime, Fraud, Hazardous materials transportation, Motor carriers, Over-the-Road bus safety, Over-the-Road buses, Public transportation, Public transportation safety, Rail hazardous materials receivers, Rail hazardous materials shippers, Rail transit systems, Railroad carriers, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures, Transportation facility, Transportation Security-Sensitive Materials.

49 CFR Part 1580

Hazardous materials transportation, Rail hazardous materials receivers, Rail hazardous materials shippers, Railroad carriers, Railroad safety, Railroads, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1582

Public transportation, Public transportation safety, Railroad carriers, Railroad safety, Railroads, Rail transit systems, Reporting and recordkeeping requirements, Security measures.

49 CFR Part 1584

Over-the-Road bus safety, Over-the-Road buses, Reporting and recordkeeping requirements, Security measures.

The Amendments

For the reasons set forth in the preamble, the Transportation Security Administration amends chapter XII, of title 49, Code of Federal Regulations as follows:

Subchapter A—Administrative and Procedural Rules

PART 1500—APPLICABILITY, TERMS, AND ABBREVIATIONS

■ 1. The authority citation for part 1500 is revised to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105; Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1408 (6 U.S.C. 1137), 1501 (6 U.S.C. 1151), 1517 (6 U.S.C. 1167), and 1534 (6 U.S.C. 1184).

■ 2. Revise § 1500.3 to read as follows:

§ 1500.3 Terms and abbreviations used in this chapter.

As used in this chapter:

Administrator means the Assistant Secretary for Homeland Security, Transportation Security Administration (Assistant Secretary), who is the highest-ranking TSA official, or his or her designee. Administrator also means the Under Secretary of Transportation for Security identified in 49 U.S.C. 114(b).

Authorized representative means any individual who is not a direct employee of a person regulated under this title, but is authorized to act on that person's behalf to perform measures required under the Transportation Security Regulations, or a TSA security program. For purposes of this subchapter, the term ''authorized representative'' includes agents, contractors, and subcontractors, and employees of the same.

Bus means any of several types of motor vehicles used by public or private entities to provide transportation service for passengers.

Bus transit system means a public transportation system providing frequent transportation service (not limited to morning and evening peak travel times) for the primary purpose of moving passengers between bus stops, often through multiple connections (a bus transit system does not become a commuter bus system even if its primary purpose is the transportation of commuters). This term does not include tourist, scenic, historic, or excursion operations.

Commuter bus system means a system providing passenger service primarily during morning and evening peak periods, between an urban area and more distant outlying communities in a greater metropolitan area. This term does not include tourist, scenic, historic, or excursion operations.

Commuter passenger train service means ''train, commuter'' as defined in 49 CFR 238.5, and includes service provided by diesel or electric powered locomotives and railroad passenger cars to serve an urban area, its suburbs, and more distant outlying communities in the greater metropolitan area. A commuter passenger train service is part of the general railroad system of transportation regardless of whether it is physically connected to other railroads.

DHS means the Department of Homeland Security and any directorate, bureau, or other component within the Department of Homeland Security, including the United States Coast Guard.

DOT means the Department of Transportation and any operating administration, entity, or office within the Department of Transportation.

Fixed-route service means the provision of transportation service by private entities operated along a prescribed route according to a fixed schedule.

General railroad system of transportation means ''the network of standard gauge track over which goods may be transported throughout the nation and passengers may travel between cities and within metropolitan and suburban areas'' as defined in appendix A to 49 CFR part 209.

Hazardous material means ''hazardous material'' as defined in 49 CFR 171.8.

Heavy rail transit means service provided by self-propelled electric railcars, typically drawing power from a third rail, operating in separate rights-of-way in multiple cars; also referred to as subways, metros or regional rail.

Host railroad means a railroad that has effective control over a segment of track.

Improvised explosive device (IED) means a device fabricated in an improvised manner that incorporates explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals in its design, and generally includes a power supply, a switch or timer, and a detonator or initiator.

Intercity passenger train service means both ''train, long-distance intercity passenger'' and ''train, short-distance intercity passenger'' as defined in 49 CFR 238.5.

Light rail transit means service provided by self-propelled electric railcars, typically drawing power from an overhead wire, operating in either exclusive or non-exclusive rights-of-way in single or multiple cars, with shorter distance trips, and frequent stops; also referred to as streetcars, trolleys, and trams.

Motor vehicle means a vehicle, machine, tractor, trailer, or semitrailer propelled or drawn by mechanical power and used upon the highways in the transportation of passengers or property, or any combination thereof, but does not include any vehicle, locomotive, or car operated exclusively on a rail or rails, or a trolley bus operated by electric power derived from a fixed overhead wire, furnishing local passenger transportation similar to street-railway service.

Over-the-Road Bus (OTRB) means a bus characterized by an elevated passenger deck located over a baggage compartment.

Owner/operator means any person that owns, or maintains operational control over, any transportation infrastructure asset, facility, or system regulated under this title, including airport operator, aircraft operator, foreign air carrier, indirect air carrier, certified cargo screening facility, flight school within the meaning of 49 CFR 1552.1(b), motor vehicle, public transportation agency, or railroad carrier. For purposes of a maritime facility or a vessel, owner/operator has

the same meaning as defined in 33 CFR 101.105.

Passenger rail car means rail rolling equipment intended to provide transportation for members of the general public and includes a self-propelled rail car designed to carry passengers, baggage, mail, or express. This term includes a rail passenger coach, cab car, and a Multiple Unit (MU) locomotive. In the context of articulated equipment, ''passenger rail car'' means that segment of the rail rolling equipment located between two trucks. This term does not include a private rail car.

Passenger railroad carrier means a railroad carrier that provides transportation to persons (other than employees, contractors, or persons riding equipment to observe or monitor railroad operations) by railroad in intercity passenger service or commuter or other short-haul passenger service in a metropolitan or suburban area.

Passenger train means a train that transports or is available to transport members of the general public.

Person means an individual, corporation, company, association, firm, partnership, society, joint-stock company, or governmental authority. It includes a trustee, receiver, assignee, successor, or similar representative of any of them.

Private rail car means rail rolling equipment that is used only for excursion, recreational, or private transportation purposes. A private rail car is not a passenger rail car.

Public transportation means transportation provided to the general public by a regular and continuing general or specific transportation vehicle that is owned or operated by a public transportation agency, including providing one or more of the following types of passenger transportation:

(1) Intercity or commuter passenger train service or other short-haul railroad passenger service in a metropolitan or suburban area (as described by 49 U.S.C. 20102(1)).

(2) Heavy or light rail transit service, whether on or off the general railroad system of transportation.

(3) An automated guideway, cable car, inclined plane, funicular, or monorail system.

(4) Bus transit or commuter bus service.

Public transportation agency means any publicly-owned or operated provider of regular and continuing public transportation.

Rail hazardous materials receiver means any owner/operator of a fixed-site facility that has a physical connection to the general railroad system of transportation and receives or unloads from transportation in commerce by rail one or more of the categories and quantities of rail security-sensitive materials identified in 49 CFR 1580.3, but does not include the owner/operator of a facility owned or operated by a department, agency or instrumentality of the Federal Government.

Rail hazardous materials shipper means the owner/operator of any fixed-site facility that has a physical connection to the general railroad system of transportation and offers (as defined in the definition of ''person who offers or offeror'' in 49 CFR 171.8), prepares or loads for transportation by rail one or more of the categories and quantities of rail security-sensitive materials as identified in 49 CFR 1580.3, but does not include the owner/operator of a facility owned or operated by a department, agency or instrumentality of the Federal Government.

Rail secure area means a secure location(s) identified by a rail hazardous materials shipper or rail hazardous materials receiver where security-related pre-transportation or transportation functions are performed or rail cars containing the categories and quantities of rail security-sensitive materials are prepared, loaded, stored, and/or unloaded.

Rail transit facility means rail transit stations, terminals, and locations at which rail transit infrastructure assets are stored, command and control operations are performed, or maintenance is performed. The term also includes rail yards, crew management centers, dispatching centers, transportation terminals and stations, fueling centers, and telecommunication centers.

Rail transit system or ''Rail Fixed Guideway System'' means any light, heavy, or rapid rail system, monorail, inclined plane, funicular, cable car, trolley, or automated guideway that traditionally does not operate on track that is part of the general railroad system of transportation.

Railroad carrier means an owner/operator providing railroad transportation.

Railroad transportation means:

(1) Any form of non-highway ground transportation that runs on rails or electromagnetic guideways, including:

(i) Commuter or other short-haul rail passenger service in a metropolitan or suburban area; and

(ii) High speed ground transportation systems that connect metropolitan areas, without regard to whether these systems use new technologies not associated with traditional railroads.

(2) Such term includes rail transit service operating on track that is part of the general railroad system of transportation but does not include rapid transit operations in an urban area that are not connected to the general railroad system of transportation.

Record includes any means by which information is preserved, irrespective of format, including a book, paper, drawing, map, recording, tape, film, photograph, machine-readable material, and any information stored in an electronic format. The term record also includes any draft, proposed, or recommended change to any record.

Sensitive security information (SSI) means information that is described in and must be managed in accordance with 49 CFR part 1520.

State means a State of the United States and the District of Columbia.

Tourist, scenic, historic, or excursion operation means a railroad or bus operation that carries passengers, often using antiquated equipment, with the conveyance of the passengers to a particular destination not being the principal purpose. Train or bus movements of new passenger equipment for demonstration purposes are not tourist, scenic, historic, or excursion operations.

Transit means mass transportation by a conveyance that provides regular and continuing general or special transportation to the public, but does not include school bus, charter, or sightseeing transportation. Rail transit may occur on or off the general railroad system of transportation.

Transportation or *transport* means the movement of property including loading, unloading, and storage. Transportation or transport also includes the movement of people, boarding, and disembarking incident to that movement.

Transportation facility means a location at which transportation cargo, equipment or infrastructure assets are stored, equipment is transferred between conveyances and/or modes of transportation, transportation command and control operations are performed, or maintenance operations are performed. The term also includes, but is not limited to, passenger stations and terminals (including any fixed facility at which passengers are picked-up or discharged), vehicle storage buildings or yards, crew management centers, dispatching centers, fueling centers, and telecommunication centers.

Transportation security equipment and systems means items, both integrated into a system and stand-alone, used by owner/operators to enhance capabilities to detect, deter,

prevent, or respond to a threat or incident, including, but not limited to, video surveillance, explosives detection, radiological detection, intrusion detection, motion detection, and security screening.

Transportation Security Regulations (TSR) means the regulations issued by the Transportation Security Administration, in title 49 of the Code of Federal Regulations, chapter XII, which includes parts 1500 through 1699.

Transportation Security-Sensitive Material (TSSM) means hazardous materials identified in 49 CFR 172.800(b).

TSA means the Transportation Security Administration.

United States, in a geographical sense, means the States of the United States, the District of Columbia, and territories and possessions of the United States, including the territorial sea and the overlying airspace.

Vulnerability assessment includes any review, audit, or other examination of the security of a transportation system, infrastructure asset, or a transportation-related automated system or network to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A vulnerability assessment includes the methodology for the assessment, the results of the assessment, and any proposed, recommended, or directed actions or countermeasures to address security concerns.

PART 1503—INVESTIGATIVE AND ENFORCEMENT PROCEDURES

■ 3. The authority citation for part 1503 continues to read as follows:

Authority: 18 U.S.C. 6002; 28 U.S.C. 2461 (note); 49 U.S.C. 114, 20109, 31105, 40113–40114, 40119, 44901–44907, 46101–46107, 46109–46110, 46301, 46305, 46311, 46313–46314; Public Law 104–134 (110 Stat. 1321; April 26, 1996), as amended by Pub. L. 114–74 (129 Stat. 584; Nov. 2, 2015); and Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1408 (6 U.S.C. 1137), 1413 (6 U.S.C. 1142), 1501 (6 U.S.C. 1151), 1512 (6 U.S.C. 1162), 1517 (6 U.S.C. 1167), 1531 (6 U.S.C. 1181), and 1534 (6 U.S.C. 1184).

Subpart B—Scope of Investigative and Enforcement Procedures

■ 4. In § 1503.101 revise paragraphs (b)(1) and (2) and add paragraph (b)(3) to read as follows:

§ 1503.101 TSA requirements.

* * * * *

(b) * * *

(1) Those provisions of title 49 U.S.C. administered by the Administrator;

(2) 46 U.S.C. chapter 701; and

(3) Provisions of Public Law 110–53 (121 Stat. 266, Aug. 3, 2007) not codified in title 49 U.S.C. that are administered by the Administrator.

Subchapter B—Security Rules for all Modes of Transportation

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

■ 5. The authority citation for part 1520 continues to read as follows:

Authority: 46 U.S.C. 114, 40113, 44901–44907, 44913–44914, 44916–44918, 44935–44936, 44942, 46105, 70102–70106, 70117; Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1408 (6 U.S.C. 1137), 1413 (6 U.S.C. 1142), 1501 (6 U.S.C. 1151), 1512 (6 U.S.C. 1162), 1517 (6 U.S.C. 1167), 1531 (6 U.S.C. 1181), and 1534 (6 U.S.C. 1184).

§ 1520.3 [Amended]

■ 6. In § 1520.3, remove the definitions of ''DHS, ''DOT'', ''Rail facility'', ''Rail hazardous materials receiver'', ''Rail hazardous materials shipper, ''Rail transit facility'', ''Rail transit system or Rail Fixed Guideway System'', ''Railroad'', ''Record'', and ''Vulnerability assessment''.

■ 7. In § 1520.5, revise paragraphs (b)(1), (b)(6)(i), (b)(8) introductory text, (b)(10), (b)(12) introductory text, and (b)(15) to read as follows:

§ 1520.5 Sensitive security information.

* * * * *

(b) * * *

(1) *Security programs, security plans, and contingency plans.* Any security program, security plan, or security contingency plan issued, established, required, received, or approved by DHS or DOT, including any comments, instructions, or implementing guidance, including—

(i) Any aircraft operator, airport operator, fixed base operator, or air cargo security program, or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103;

(iv) Any security incident response plan established under 46 U.S.C. 70104, and

(v) Any security program or plan required under subchapter D of this title.

* * * * *

(6) * * *

(i) Details of any aviation, maritime, or surface transportation inspection, or any investigation or an alleged violation of aviation, maritime, or surface transportation security requirements of Federal law, that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or investigation, and including any recommendations concerning the inspection or investigation.

* * * * *

(8) *Security measures.* Specific details of aviation, maritime, or surface transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including the following:

* * * * *

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out aviation, maritime, or surface transportation security measures required or recommended by DHS or DOT.

* * * * *

(12) *Critical transportation infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or surface transportation that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

* * * * *

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation, maritime, or surface transportation, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.

* * * * *

■ 8. In § 1520.7, revise paragraph (n) to read as follows:

§ 1520.7 Covered persons.

* * * * *

(n) Each owner/operator of maritime or surface transportation subject to the requirements of subchapter D of this chapter.

■ 9. Revise the heading for subchapter D to read as follows:

Subchapter D—Maritime and Surface Transportation Security

■ 10. Revise part 1570 to read as follows:

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).

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 means any person not a citizen or national of the United States.

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.

Lawful permanent resident means an alien lawfully admitted for permanent residence, as defined in 8 U.S.C. 1101(a)(20).

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.

National of the United States means a citizen of the United States, or a person who, though not a citizen, owes permanent allegiance to the United States, as defined in 8 U.S.C. 1101(a)(22), and includes American Samoa and Swains Island.

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.

Security threat means an individual whom TSA determines or suspects of posing a threat to national security; to transportation security; or of terrorism.

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.

§ 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 Compliance, inspection, and enforcement.

(a) Each person subject to any of the requirements of this subchapter, must allow TSA and other authorized DHS officials, at any time and in a reasonable manner, without advance notice, to enter, assess, inspect, and test property, facilities, equipment, and operations; and to view, inspect, and copy records, as necessary to carry out TSA's security-related statutory or regulatory authorities, including its authority to—

(1) Assess threats to transportation.

(2) Enforce security-related laws, regulations, directives, and requirements.

(3) Inspect, maintain, and test the security of facilities, equipment, and systems.

(4) Ensure the adequacy of security measures for the transportation of passengers and cargo.

(5) Oversee the implementation, and ensure the adequacy, of security measures for the owner/operator's conveyances and vehicles, at transportation facilities and infrastructure and other assets related to transportation.

(6) Review security plans and/or programs.

(7) Determine compliance with any requirements in this chapter.

(8) Carry out such other duties, and exercise such other powers, relating to transportation security, as the Administrator for TSA considers appropriate, to the extent authorized by law.

(b) At the request of TSA, each owner/operator subject to the requirements of this subchapter must provide evidence of compliance with this chapter, including copies of records.

(c) TSA and other authorized DHS officials, may enter, without advance notice, and be present within any area or within any vehicle or conveyance, terminal, or other facility covered by this chapter without access media or identification media issued or approved by an owner/operator covered by this chapter in order to inspect or test compliance, or perform other such duties as TSA may direct.

(d) TSA inspectors and other authorized DHS officials working with TSA will, on request, present their credentials for examination, but the credentials may not be photocopied or otherwise reproduced.

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 90 calendar days after June 22, 2020.

(2) If commencing or modifying operations so as to be subject to the requirements of subpart B to 49 CFR part 1580, 1582, or 1584 after June 22, 2020, 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.

§ 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—

(1) No later than one year after the date of TSA-approval of the owner/operator's security training program if the employee is employed to perform a security-sensitive function on the date TSA approves the program.

(2) No later than 60 calendar days after the employee first performs a security-sensitive job function if performance of a security-sensitive job function is initiated after TSA approves the security training program.

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

(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.

§ 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) 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.

(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.

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).
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).

Category	Description
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).

■ 11. Revise part 1580 to read as follows:

PART 1580—FREIGHT RAIL TRANSPORTATION SECURITY

Subpart A—General

Sec.
1580.1 Scope.
1580.3 Terms used in this part.
1580.5 Preemptive effect.

Subpart B—Security Programs

1580.101 Applicability.
1580.103 [Reserved]
1580.105 [Reserved]
1580.107 [Reserved]
1580.109 [Reserved]
1580.111 [Reserved]
1580.113 Security training program general requirements.
1580.115 Security training and knowledge for security-sensitive employees.

Subpart C—Operations

1580.201 Applicability.
1580.203 Location and shipping information.
1580.205 Chain of custody and control requirements.
1580.207 Harmonization of Federal regulation of nuclear facilities.
Appendix A to Part 1580—High Threat Urban Areas (HTUAS)
Appendix B to Part 1580—Security-Sensitive Job Functions for Freight Rail

Authority: 49 U.S.C. 114; Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1501 (6 U.S.C. 1151), 1512 (6 U.S.C. 1162) and 1517 (6 U.S.C. 1167).

Subpart A—General

§ 1580.1 Scope.

(a) Except as provided in paragraph (b) of this section, this part includes requirements for the following persons. Specific sections in this part provide detailed requirements.

(1) Each freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.

(2) Each rail hazardous materials shipper.

(3) Each rail hazardous materials receiver located within an HTUA.

(4) Each freight railroad carrier serving as a host railroad to a freight railroad operation described in paragraph (a)(1) of this section or a passenger operation described in § 1582.1 of this subchapter.

(5) Each owner/operator of private rail cars, including business/office cars and circus trains, on or connected to the general railroad system of transportation.

(b) This part does not apply to a freight railroad carrier that operates rolling equipment only on track inside an installation that is not part of the general railroad system of transportation.

§ 1580.3 Terms used in this part.

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 terms apply to this part:

Class I means Class I as assigned by regulations of the Surface Transportation Board (STB) (49 CFR part 1201; General Instructions 1–1).

Attended, in reference to a rail car, means an employee—

(1) Is physically located on-site in reasonable proximity to the rail car;

(2) Is capable of promptly responding to unauthorized access or activity at or near the rail car, including immediately contacting law enforcement or other authorities; and

(3) Immediately responds to any unauthorized access or activity at or near the rail car either personally or by contacting law enforcement or other authorities.

Document the transfer means documentation uniquely identifying that the rail car was attended during the transfer of custody, including:

(1) Car initial and number.

(2) Identification of individuals who attended the transfer (names or uniquely identifying employee number).

(3) Location of transfer.

(4) Date and time the transfer was completed.

High threat urban area (HTUA) means, for purposes of this part, an area comprising one or more cities and surrounding areas including a 10-mile buffer zone, as listed in appendix A to this part 1580.

Maintains positive control means that the rail hazardous materials receiver

and the railroad carrier communicate and cooperate with each other to provide for the security of the rail car during the physical transfer of custody. *Attending* the rail car is a component of maintaining positive control.

Rail security-sensitive materials (RSSM) means—

(1) A rail car containing more than 2,268 kg (5,000 lbs.) of a Division 1.1, 1.2, or 1.3 (explosive) material, as defined in 49 CFR 173.50;

(2) A tank car containing a material poisonous by inhalation as defined in 49 CFR 171.8, including anhydrous ammonia, Division 2.3 gases poisonous by inhalation as set forth in 49 CFR 173.115(c), and Division 6.1 liquids meeting the defining criteria in 49 CFR 173.132(a)(1)(iii) and assigned to hazard zone A or hazard zone B in accordance with 49 CFR 173.133(a), excluding residue quantities of these materials; and

(3) A rail car containing a highway route-controlled quantity of a Class 7 (radioactive) material, as defined in 49 CFR 173.403.

Residue means the hazardous material remaining in a packaging, including a tank car, after its contents have been unloaded to the maximum extent practicable and before the packaging is either refilled or cleaned of hazardous material and purged to remove any hazardous vapors.

Security-sensitive employee means an employee who performs—

(1) Service subject to the Federal hours of service laws (49 U.S.C. chapter 211), regardless of whether the employee actually performs such service during a particular duty tour; or

(2) One or more of the security-sensitive job functions identified in Appendix B to this part where the security-sensitive function is performed in the United States or in direct support of the common carriage of persons or property between a place in the United States and any place outside of the United States.

§ 1580.5 Preemptive effect.

Under 49 U.S.C. 20106, issuance of the regulations in this subchapter preempts any State law, regulation, or order covering the same subject matter, except an additional or more stringent law, regulation, or order that is necessary to eliminate or reduce an essentially local security hazard; that is not incompatible with a law, regulation, or order of the U.S. Government; and that does not unreasonably burden interstate commerce. For example, under 49 U.S.C. 20106, issuance of 49 CFR 1580.205 preempts any State or tribal law, rule, regulation, order or common law requirement covering the same subject matter.

Subpart B—Security Programs

§ 1580.101 Applicability.

This subpart applies to each of the following owner/operators:

(a) Described in § 1580.1(a)(1) of this part that is a Class I freight railroad.

(b) Described in § 1580.1(a)(1) of this part that transports one or more of the categories and quantities of RSSM in an HTUA.

(c) Described in § 1580.1(a)(4) of this part that serves as a host railroad to a freight railroad described in paragraph (a) of (b) of this section or a passenger operation described in § 1582.101 of this subchapter.

§ 1580.103 [Reserved]

§ 1580.105 [Reserved]

§ 1580.107 [Reserved]

§ 1580.109 [Reserved]

§ 1580.111 [Reserved]

§ 1580.113 Security training program general requirements.

(a) *Security training program required.* Each owner/operator identified in § 1580.101 of this part is required to adopt and carry out a security training program under this subpart.

(b) *General requirements.* The security training program must include the following information:

(1) Name of owner/operator.

(2) Name, title, telephone number, and email address of the primary individual to be contacted with regard to review of the security training program.

(3) Number, by specific job function category identified in Appendix B to this part, of security-sensitive employees trained or to be trained.

(4) Implementation schedule that identifies a specific date by which initial and recurrent security training required by § 1570.111 of this subchapter will be completed.

(5) Location where training program records will be maintained.

(6) Curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements of § 1580.115 of this part. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under § 1570.111 of this subchapter is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(7) Plan for ensuring supervision of untrained security-sensitive employees performing functions identified in Appendix B to this part.

(8) Plan for notifying employees of changes to security measures that could change information provided in previously provided training.

(9) Method(s) for evaluating the effectiveness of the security training program in each area required by § 1580.115 of this part.

(c) *Relation to other training.* (1) Training conducted by owner/operators to comply other requirements or standards, such as emergency preparedness training required by the Department of Transportation (DOT) (49 CFR part 239) or other training for communicating with emergency responders to arrange the evacuation of passengers, may be combined with and used to satisfy elements of the training requirements in this subpart.

(2) If the owner/operator submits a security training program that relies on pre-existing or previous training materials to meet the requirements of subpart B, the program submitted for approval must include an index, organized in the same sequence as the requirements in this subpart.

(d) *Submission and implementation.* The owner/operator must submit and implement the security training program in accordance with the schedules identified in §§ 1570.109 and 1570.111 of this subchapter.

§ 1580.115 Security training and knowledge for security-sensitive employees.

(a) *Training required for security-sensitive employees.* No owner/operator required to have a security training program under § 1580.101 of this part may use a security-sensitive employee to perform a function identified in Appendix B to this part, unless that individual has received training as part of a security training program approved by TSA under 49 CFR part 1570, subpart B, or is under the direct supervision of an employee who has received the training required by this section as applicable to that security-sensitive function.

(b) *Limits on use of untrained employees.* Notwithstanding paragraph (a) of this section, a security-sensitive employee may not perform a security-sensitive function for more than sixty (60) calendar days without receiving security training.

(c) *Prepare.* (1) Each owner/operator must ensure that each of its security-sensitive employees with position- or

function-specific responsibilities under the owner/operator's security program has knowledge of how to fulfill those responsibilities in the event of a security threat, breach, or incident to ensure—

(i) Employees with responsibility for transportation security equipment and systems are aware of their responsibilities and can verify the equipment and systems are operating and properly maintained; and

(ii) Employees with other duties and responsibilities under the company's security plans and/or programs, including those required by Federal law, know their assignments and the steps or resources needed to fulfill them.

(2) Each employee who performs any security-related functions under § 1580.205 of this subpart must be provided training specifically applicable to the functions the employee performs. As applicable, this training must address—

(i) Inspecting rail cars for signs of tampering or compromise, IEDs, suspicious items, and items that do not belong;

(ii) Identification of rail cars that contain rail security-sensitive materials, including the owner/operator's procedures for identifying rail security-sensitive material cars on train documents, shipping papers, and in computer train/car management systems; and

(iii) Procedures for completing transfer of custody documentation.

(d) *Observe.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of the observational skills necessary to recognize—

(1) Suspicious and/or dangerous items (such as substances, packages, or conditions (for example, characteristics of an IED and signs of equipment tampering or sabotage);

(2) Combinations of actions and individual behaviors that appear suspicious and/or dangerous, inappropriate, inconsistent, or out of the ordinary for the employee's work environment, which could indicate a threat to transportation security; and

(3) How a terrorist or someone with malicious intent may attempt to gain sensitive information or take advantage of vulnerabilities.

(e) *Assess.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge necessary to—

(1) Determine whether the item, individual, behavior, or situation requires a response as a potential terrorist threat based on the respective transportation environment; and

(2) Identify appropriate responses based on observations and context.

(f) *Respond.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of how to—

(1) Appropriately report a security threat, including knowing how and when to report internally to other employees, supervisors, or management, and externally to local, state, or Federal agencies according to the owner/operator's security procedures or other relevant plans;

(2) Interact with the public and first responders at the scene of the threat or incident, including communication with passengers on evacuation and any specific procedures for individuals with disabilities and the elderly; and

(3) Use any applicable self-defense devices or other protective equipment provided to employees by the owner/operator.

Subpart C—Operations

§ 1580.201 Applicability.

This subpart applies to the following:

(1) Each owner/operator described in § 1580.1(a)(1) of this part that transports one or more of the categories and quantities of rail security-sensitive materials.

(2) Each owner/operator described in § 1580.1(a)(2) and (3) of this part.

§ 1580.203 Location and shipping information.

(a) *General requirement.* Each owner/operator described in § 1580.201 of this part must have procedures in place to determine the location and shipping information for each rail car under its physical custody and control that contains one or more of the categories and quantities of rail security-sensitive materials.

(b) *Required information.* The location and shipping information must include the following:

(1) The rail car's current location by city, county, and state, including, for freight railroad carriers, the railroad milepost, track designation, and the time that the rail car's location was determined.

(2) The rail car's routing, if a freight railroad carrier.

(3) A list of the total number of rail cars containing rail security-sensitive materials, broken down by—

(i) The shipping name prescribed for the material in column 2 of the table in 49 CFR 172.101;

(ii) The hazard class or division number prescribed for the material in column 3 of the table in 49 CFR 172.101; and

(iii) The identification number prescribed for the material in column 4 of the table in 49 CFR 172.101.

(4) Each rail car's initial and number.

(5) Whether the rail car is in a train, rail yard, siding, rail spur, or rail hazardous materials shipper or receiver facility, including the name of the rail yard or siding designation.

(c) *Timing-Class I freight railroad carriers.* Upon request by TSA, each Class I freight railroad carrier described in paragraph (a) of this section must provide the location and shipping information to TSA no later than—

(1) Five minutes if the request applies to a single (one) rail car; and

(2) Thirty minutes if the request concerns multiple rail cars or a geographic region.

(d) *Timing-other than Class I freight railroad carriers.* Upon request by TSA, all owner/operators described in paragraph (a) of this section, other than Class I freight railroad carriers, must provide the location and shipping information to TSA no later than 30 minutes, regardless of the number of cars covered by the request.

(e) *Method.* All owner/operators described in paragraph (a) of this section must provide the requested location and shipping information to TSA by one of the following methods:

(1) Electronic data transmission in spreadsheet format.

(2) Electronic data transmission in Hyper Text Markup Language (HTML) format.

(3) Electronic data transmission in Extensible Markup Language (XML).

(4) Facsimile transmission of a hard copy spreadsheet in tabular format.

(5) Posting the information to a secure website address approved by TSA.

(6) Another format approved by TSA.

(f) *Telephone number.* Each owner/operator described in § 1580.201 of this part must provide a telephone number for use by TSA to request the information required in paragraph (b) of this section.

(1) The telephone number must be monitored at all times.

(2) A telephone number that requires a call back (such as an answering service, answering machine, or beeper device) does not meet the requirements of this paragraph.

§ 1580.205 Chain of custody and control requirements.

(a) *Within or outside of an HTUA, rail hazardous materials shipper transferring to carrier.* Except as provided in paragraph (g) of this section, at each location within or outside of an HTUA, a rail hazardous materials shipper transferring custody of

a rail car containing one or more of the categories and quantities of rail security-sensitive materials to a freight railroad carrier must do the following:

(1) Physically inspect the rail car before loading for signs of tampering, including closures and seals; other signs that the security of the car may have been compromised; and suspicious items or items that do not belong, including the presence of an improvised explosive device.

(2) Keep the rail car in a rail secure area from the time the security inspection required by paragraph (a)(1) of this section or by 49 CFR 173.31(d), whichever occurs first, until the freight railroad carrier takes physical custody of the rail car.

(3) Document the transfer of custody to the railroad carrier in hard copy or electronically.

(b) *Within or outside of an HTUA, carrier receiving from a rail hazardous materials shipper.* At each location within or outside of an HTUA where a freight railroad carrier receives from a rail hazardous materials shipper custody of a rail car containing one or more of the categories and quantities of rail security-sensitive materials, the freight railroad carrier must document the transfer in hard copy or electronically and perform the required security inspection in accordance with 49 CFR 174.9.

(c) *Within an HTUA, carrier transferring to carrier.* Within an HTUA, whenever a freight railroad carrier transfers a rail car containing one or more of the categories and quantities of rail security-sensitive materials to another freight railroad carrier, each freight railroad carrier must adopt and carry out procedures to ensure that the rail car is not left unattended at any time during the physical transfer of custody. These procedures must include the receiving freight railroad carrier performing the required security inspection in accordance with 49 CFR 174.9. Both the transferring and the receiving railroad carrier must document the transfer of custody in hard copy or electronically.

(d) *Outside of an HTUA, carrier transferring to carrier.* Outside an HTUA, whenever a freight railroad carrier transfers a rail car containing one or more of the categories and quantities of rail security-sensitive materials to another freight railroad carrier, and the rail car containing this hazardous material may subsequently enter an HTUA, each freight railroad carrier must adopt and carry out procedures to ensure that the rail car is not left unattended at any time during the physical transfer of custody. These procedures must include the receiving railroad carrier performing the required security inspection in accordance with 49 CFR 174.9. Both the transferring and the receiving railroad carrier must document the transfer of custody in hard copy or electronically.

(e) *Within an HTUA, carrier transferring to rail hazardous materials receiver.* A freight railroad carrier delivering a rail car containing one or more of the categories and quantities of rail security-sensitive materials to a rail hazardous materials receiver located within an HTUA must not leave the rail car unattended in a non-secure area until the rail hazardous materials receiver accepts custody of the rail car. Both the railroad carrier and the rail hazardous materials receiver must document the transfer of custody in hard copy or electronically.

(f) *Within an HTUA, rail hazardous materials receiver receiving from carrier.* Except as provided in paragraph (j) of this section, a rail hazardous materials receiver located within an HTUA that receives a rail car containing one or more of the categories and quantities of rail security-sensitive materials from a freight railroad carrier must—

(1) Ensure that the rail hazardous materials receiver or railroad carrier maintains positive control of the rail car during the physical transfer of custody of the rail car;

(2) Keep the rail car in a rail secure area until the car is unloaded; and

(3) Document the transfer of custody from the railroad carrier in hard copy or electronically.

(g) *Within or outside of an HTUA, rail hazardous materials receiver rejecting car.* This section does not apply to a rail hazardous materials receiver that does not routinely offer, prepare, or load for transportation by rail one or more of the categories and quantities of rail security-sensitive materials. If such a receiver rejects and returns a rail car containing one or more of the categories and quantities of rail security-sensitive materials to the originating offeror or shipper, the requirements of this section do not apply to the receiver. The requirements of this section do apply to any railroad carrier to which the receiver transfers custody of the rail car.

(h) *Document retention.* Covered entities must maintain the documents required under this section for at least 60 calendar days and make them available to TSA upon request.

(i) *Rail secure area.* The rail hazardous materials shipper and the rail hazardous materials receiver must use physical security measures to ensure that no unauthorized individual gains access to the rail secure area.

(j) *Exemption for rail hazardous materials receivers.* A rail hazardous materials receiver located within an HTUA may request from TSA an exemption from some or all of the requirements of this section if the receiver demonstrates that the potential risk from its activities is insufficient to warrant compliance with this section. TSA will consider all relevant circumstances, including the following:

(1) The amounts and types of all hazardous materials received.

(2) The geography of the area surrounding the receiver's facility.

(3) Proximity to entities that may be attractive targets, including other businesses, housing, schools, and hospitals.

(4) Any information regarding threats to the facility.

(5) Other circumstances that indicate the potential risk of the receiver's facility does not warrant compliance with this section.

§ 1580.207 Harmonization of Federal regulation of nuclear facilities.

TSA will coordinate activities under this subpart with the Nuclear Regulatory Commission (NRC) and the Department of Energy (DOE) with respect to regulation of rail hazardous materials shippers and receivers that are also licensed or regulated by the NRC or DOE under the Atomic Energy Act of 1954, as amended, to maintain consistency with the requirements imposed by the NRC and DOE.

Appendix A to Part 1580—High Threat Urban Areas (HTUAs)

State	Urban area	Geographic areas
AZ	Phoenix Area	Chandler, Gilbert, Glendale, Mesa, Peoria, Phoenix, Scottsdale, Tempe, and a 10-mile buffer extending from the border of the combined area.
CA	Anaheim/Santa Ana Area.	Anaheim, Costa Mesa, Garden Grove, Fullerton, Huntington Beach, Irvine, Orange, Santa Ana, and a 10-mile buffer extending from the border of the combined area.

State	Urban area	Geographic areas
	Bay Area	Berkeley, Daly City, Fremont, Hayward, Oakland, Palo Alto, Richmond, San Francisco, San Jose, Santa Clara, Sunnyvale, Vallejo, and a 10-mile buffer extending from the border of the combined area.
	Los Angeles/Long Beach Area.	Burbank, Glendale, Inglewood, Long Beach, Los Angeles, Pasadena, Santa Monica, Santa Clarita, Torrance, Simi Valley, Thousand Oaks, and a 10-mile buffer extending from the border of the combined area.
	Sacramento Area	Elk Grove, Sacramento, and a 10-mile buffer extending from the border of the combined area.
	San Diego Area	Chula Vista, Escondido, and San Diego, and a 10-mile buffer extending from the border of the combined area.
CO	Denver Area	Arvada, Aurora, Denver, Lakewood, Westminster, Thornton, and a 10-mile buffer extending from the border of the combined area.
DC	National Capital Region	National Capital Region and a 10-mile buffer extending from the border of the combined area.
FL	Fort Lauderdale Area	Fort Lauderdale, Hollywood, Miami Gardens, Miramar, Pembroke Pines, and a 10-mile buffer extending from the border of the combined area.
	Jacksonville Area	Jacksonville and a 10-mile buffer extending from the city border.
	Miami Area	Hialeah, Miami, and a 10-mile buffer extending from the border of the combined area.
	Orlando Area	Orlando and a 10-mile buffer extending from the city border.
	Tampa Area	Clearwater, St. Petersburg, Tampa, and a 10-mile buffer extending from the border of the combined area.
GA	Atlanta Area	Atlanta and a 10-mile buffer extending from the city border.
HI	Honolulu Area	Honolulu and a 10-mile buffer extending from the city border.
IL	Chicago Area	Chicago and a 10-mile buffer extending from the city border.
IN	Indianapolis Area	Indianapolis and a 10-mile buffer extending from the city border.
KY	Louisville Area	Louisville and a 10-mile buffer extending from the city border.
LA	Baton Rouge Area	Baton Rouge and a 10-mile buffer extending from the city border.
	New Orleans Area	New Orleans and a 10-mile buffer extending from the city border.
MA	Boston Area	Boston, Cambridge, and a 10-mile buffer extending from the border of the combined area.
MD	Baltimore Area	Baltimore and a 10-mile buffer extending from the city border.
MI	Detroit Area	Detroit, Sterling Heights, Warren, and a 10-mile buffer extending from the border of the combined area.
MN	Twin Cities Area	Minneapolis, St. Paul, and a 10-mile buffer extending from the border of the combined entity.
MO	Kansas City Area	Independence, Kansas City (MO), Kansas City (KS), Olathe, Overland Park, and a 10-mile buffer extending from the border of the combined area.
	St. Louis Area	St. Louis and a 10-mile buffer extending from the city border.
NC	Charlotte Area	Charlotte and a 10-mile buffer extending from the city border.
NE	Omaha Area	Omaha and a 10-mile buffer extending from the city border.
NJ	Jersey City/Newark Area.	Elizabeth, Jersey City, Newark, and a 10-mile buffer extending from the border of the combined area.
NV	Las Vegas Area	Las Vegas, North Las Vegas, and a 10-mile buffer extending from the border of the combined entity.
NY	Buffalo Area	Buffalo and a 10-mile buffer extending from the city border.
	New York City Area	New York City, Yonkers, and a 10-mile buffer extending from the border of the combined area.
OH	Cincinnati Area	Cincinnati and a 10-mile buffer extending from the city border.
	Cleveland Area	Cleveland and a 10-mile buffer extending from the city border.
	Columbus Area	Columbus and a 10-mile buffer extending from the city border.
	Toledo Area	Oregon, Toledo, and a 10-mile buffer extending from the border of the combined area.
OK	Oklahoma City Area	Norman, Oklahoma and a 10-mile buffer extending from the border of the combined area.
OR	Portland Area	Portland, Vancouver, and a 10-mile buffer extending from the border of the combined area.
PA	Philadelphia Area	Philadelphia and a 10-mile buffer extending from the city border.
	Pittsburgh Area	Pittsburgh and a 10-mile buffer extending from the city border.
TN	Memphis Area	Memphis and a 10-mile buffer extending from the city border.
TX	Dallas/Fort Worth/Arlington Area.	Arlington, Carrollton, Dallas, Fort Worth, Garland, Grand Prairie, Irving, Mesquite, Plano, and a 10-mile buffer extending from the border of the combined area.
	Houston Area	Houston, Pasadena, and a 10-mile buffer extending from the border of the combined entity.
	San Antonio Area	San Antonio and a 10-mile buffer extending from the city border.
WA	Seattle Area	Seattle, Bellevue, and a 10-mile buffer extending from the border of the combined area.
WI	Milwaukee Area	Milwaukee and a 10-mile buffer extending from the city border.

Appendix B to Part 1580—Security-Sensitive Functions for Freight Rail

This table identifies security-sensitive job functions for owner/operators regulated under this part. All employees performing security-sensitive functions are ''security-sensitive employees'' for purposes of this rule and must be trained.

Categories	Security-sensitive job functions for freight rail	Examples of job titles applicable to these functions*
A. Operating a vehicle	1. Employees who operate or directly control the movements of locomotives or other self-powered rail vehicles.	Engineer, conductor

Categories	Security-sensitive job functions for freight rail	Examples of job titles applicable to these functions *
	2. Train conductor, trainman, brakeman, or utility employee or performs acceptance inspections, couples and uncouples rail cars, applies handbrakes, or similar functions. 3. Employees covered under the Federal hours of service laws as ''train employees.'' *See* 49 U.S.C. 21101(5) and 21103..	
B. Inspecting and maintaining vehicles	Employees who inspect or repair rail cars and locomotives.	Carman, car repairman, car inspector, engineer, conductor.
C. Inspecting or maintaining building or transportation infrastructure	1. Employees who— a. Maintain, install, or inspect communications and signal equipment. b. Maintain, install, or inspect track and structures, including, but not limited to, bridges, trestles, and tunnels. 2. Employees covered under the Federal hours of service laws as ''signal employees.'' *See* 49 U.S.C. 21101(3) and 21104.	Signalman, signal maintainer, track-man, gang foreman, bridge and building laborer, roadmaster, bridge, and building inspector/operator.
D. Controlling dispatch or movement of a vehicle	1. Employees who— a. Dispatch, direct, or control the movement of trains. b. Operate or supervise the operations of moveable bridges. c. Supervise the activities of train crews, car movements, and switching operations in a yard or terminal. 2. Employees covered under the Federal hours of service laws as ''dispatching service employees.'' *See* 49 U.S.C. 21101(2) and 21105.	Yardmaster, dispatcher, block operator, bridge operator.
E. Providing security of the owner/operator's equipment and property	Employees who provide for the security of the railroad carrier's equipment and property, including acting as a railroad police officer (as that term is defined in 49 CFR 207.2).	Police officer, special agent; patrolman; watchman; guard.
F. Loading or unloading cargo or baggage	Includes, but is not limited to, employees that load or unload hazardous materials.	Service track employee.
G. Interacting with travelling public (on board a vehicle or within a transportation facility).	Employees of a freight railroad operating in passenger service.	Conductor, engineer, agent.
H. Complying with security programs or measures, including those required by Federal law.	1. Employees who serve as security coordinators designated in § 1570.201 of this subchapter, as well as any designated alternates or secondary security coordinators. 2. Employees who—. a. Conduct training and testing of employees when the training or testing is required by TSA's security regulations. b. Perform inspections or operations required by § 1580.205 of this subchapter. c. Manage or direct implementation of security plan requirements.	Security coordinator, train master, assistant train master, roadmaster, division roadmaster.

* These job titles are provided solely as a resource to help understand the functions described; whether an employee must be trained is based upon the function, not the job title.

■ 12. Add part 1582 to read as follows:

PART 1582—PUBLIC TRANSPORTATION AND PASSENGER RAILROAD SECURITY

Subpart A—General

Sec.

Subpart B—Security Programs

Authority: 49 U.S.C. 114; Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1402 (6 U.S.C. 1131), 1405 (6 U.S.C. 1134), and 1408 (6 U.S.C. 1137).

Subpart A—General

§ 1582.1 Scope.

(a) Except as provided in paragraph (b) of this section, this part includes requirements for the following persons. Specific sections in this part provide detailed requirements.

(1) Each passenger railroad carrier.

(2) Each public transportation agency.

(3) Each operator of a rail transit system that is not operating on track that is part of the general railroad system of transportation, including heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems.

(4) Each tourist, scenic, historic, and excursion rail owner/operator, whether operating on or off the general railroad system of transportation.

(b) This part does not apply to a ferry system required to conduct training pursuant to 46 U.S.C. 70103.

§ 1582.3 Terms used in this part.

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-sensitive employee means an employee whose responsibilities for the owner/operator include one or more of the security-sensitive job functions identified in appendix B to this part if the security-sensitive function is performed in the United States or in direct support of the common carriage of persons or property between a place in the United States and any place outside of the United States.

§ 1582.5 Preemptive effect.

Under 49 U.S.C. 20106, issuance of the passenger railroad and public transportation regulations in this subchapter preempts any State law, regulation, or order covering the same subject matter, except an additional or more stringent law, regulation, or order that is necessary to eliminate or reduce an essentially local security hazard; that is not incompatible with a law, regulation, or order of the U.S. Government; and that does not unreasonably burden interstate commerce.

Subpart B—Security Programs

§ 1582.101 Applicability.

The requirements of this subpart apply to the following:

(a) Amtrak (also known as the National Railroad Passenger Corporation).

(b) Each owner/operator identified in Appendix A to this part.

(c) Each owner/operator described in § 1582.1(a)(1) through (3) of this part that serves as a host railroad to a freight operation described in § 1580.301 of this subchapter or to a passenger train operation described in paragraph (a)(1) or (a)(2) of this section.

§ 1582.103 [Reserved]

§ 1582.105 [Reserved]

§ 1582.107 [Reserved]

§ 1582.109 [Reserved]

§ 1582.111 [Reserved]

§ 1582.113 Security training program general requirements.

(a) *Security training program required.* Each owner/operator identified in § 1582.101 of this part is required to adopt and carry out a security training program under this subpart.

(b) *General requirements.* The security training program must include the following information:

(1) Name of owner/operator.

(2) Name, title, telephone number, and email address of the primary individual to be contacted with regard to review of the security training program.

(3) Number, by specific job function category identified in Appendix B to this part, of security-sensitive employees trained or to be trained.

(4) Implementation schedule that identifies a specific date by which initial and recurrent security training required by § 1570.111 of this subchapter will be completed.

(5) Location where training program records will be maintained.

(6) Curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements of § 1582.115 of this part. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under § 1570.111 of this subchapter is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(7) Plan for ensuring supervision of untrained security-sensitive employees performing functions identified in Appendix B to this part.

(8) Plan for notifying employees of changes to security measures that could change information provided in previously provided training.

(9) Method(s) for evaluating the effectiveness of the security training program in each area required by § 1582.115 of this part.

(c) *Relation to other training.* (1) Training conducted by owner/operators to comply other requirements or standards, such as emergency preparedness training required by the Department of Transportation (DOT) (49 CFR part 239) or other training for communicating with emergency responders to arrange the evacuation of passengers, may be combined with and used to satisfy elements of the training requirements in this subpart.

(2) If the owner/operator submits a security training program that relies on pre-existing or previous training materials to meet the requirements of subpart B, the program submitted for approval must include an index, organized in the same sequence as the requirements in this subpart.

(d) *Submission and implementation.* The owner/operator must submit and implement the security training program in accordance with the schedules identified in §§ 1570.109 and 1570.111 of this subchapter.

§ 1582.115 Security training and knowledge for security-sensitive employees.

(a) *Training required for security-sensitive employees.* No owner/operator required to have a security training program under § 1582.101 of this part may use a security-sensitive employee to perform a function identified in appendix B to this part unless that individual has received training as part of a security training program approved by TSA under 49 CFR part 1570, subpart B, or is under the direct supervision of an employee who has received the training required by this section as applicable to that security-sensitive function.

(b) *Limits on use of untrained employees.* Notwithstanding paragraph (a) of this section, a security-sensitive employee may not perform a security-sensitive function for more than sixty (60) calendar days without receiving security training.

(c) *Prepare.* Each owner/operator must ensure that each of its security-sensitive employees with position- or function-specific responsibilities under the owner/operator's security program have knowledge of how to fulfill those

responsibilities in the event of a security threat, breach, or incident to ensure—

(1) Employees with responsibility for transportation security equipment and systems are aware of their responsibilities and can verify the equipment and systems are operating and properly maintained; and

(2) Employees with other duties and responsibilities under the company's security plans and/or programs, including those required by Federal law, know their assignments and the steps or resources needed to fulfill them.

(d) *Observe.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of the observational skills necessary to recognize—

(1) Suspicious and/or dangerous items (such as substances, packages, or conditions (for example, characteristics of an IED and signs of equipment tampering or sabotage);

(2) Combinations of actions and individual behaviors that appear suspicious and/or dangerous, inappropriate, inconsistent, or out of the ordinary for the employee's work environment, which could indicate a threat to transportation security; and

(3) How a terrorist or someone with malicious intent may attempt to gain sensitive information or take advantage of vulnerabilities.

(e) *Assess.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge necessary to—

(1) Determine whether the item, individual, behavior, or situation requires a response as a potential terrorist threat based on the respective transportation environment; and

(2) Identify appropriate responses based on observations and context.

(f) *Respond.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of how to—

(1) Appropriately report a security threat, including knowing how and when to report internally to other employees, supervisors, or management, and externally to local, state, or Federal agencies according to the owner/operator's security procedures or other relevant plans;

(2) Interact with the public and first responders at the scene of the threat or incident, including communication with passengers on evacuation and any specific procedures for individuals with disabilities and the elderly; and

(3) Use any applicable self-defense devices or other protective equipment provided to employees by the owner/operator.

Appendix A to Part 1582—Determinations for Public Transportation and Passenger Railroads

State	Urban area	Systems
CA	Bay Area	Alameda-Contra Costa Transit District (AC Transit).
		Altamont -Corridor Express (ACE).
		City and County of San Francisco (San Francisco Bay Area Rapid Transit District) (BART).
		Central Contra Costa Transit Authority.
		≤Golden Gate Bridge, Highway and Transportation District (GGBHTD).
		Peninsula Corridor Joint Powers Board (PCJPB) (Caltrain).
		San Francisco Municipal Railway (MUNI) (San Francisco Municipal Transportation Agency).
		San Mateo County Transit District (San Mateo County Transit Authority) (SamTrans).
		Santa Clara Valley Transportation Authority (VTA).
		Transbay Joint Powers Authority.
	Greater Los Angeles Area (Los Angeles/Long Beach and Anaheim/Santa Ana urban Areas)..	City of Los Angeles Department of Transportation (LADOT)
		Foothill Transit.
		Long Beach Transit (LBT).
		Los Angeles County Metropolitan Transportation Authority (LACMTA).
		City of Montebello (Montebello Bus Lines) (MBL).
		Omnitrans (OMNI).
		Orange County Transportation Authority (OCTA).
		City of Santa Monica (Santa Monica's Big Blue Bus) (Big Blue Bus).
		Southern California Regional Rail Authority (Metrolink).
DC/MD/VA	Greater National Capital Region (National Capital Region and Baltimore urban Areas)..	Arlington County, Virginia (Arlington Transit).
		City of Alexandria (Alexandria Transit Company) (Dash).
		Fairfax County Department of Transportation—Fairfax Connector Bus System.
		Maryland Transit Administration (MTA).
		Montgomery County Department of Transportation (Ride-On Montgomery County Transit).
		Potomac and Rappahannock Transportation Commission.
		Prince George's County Department of Public Works and Transportation (The Bus).
		Virginia Railway Express (VRE).
		Washington Metropolitan Area Transit Authority (WMATA).
GA	Atlanta Area	Georgia Regional Transportation Authority (GRTA, within State Road and Tollway Authority (SRTA)).
Metropolitan Atlanta Rapid Transit Authority (MARTA)..		
IL/IN	Chicago Area	Chicago Transit Authority (CTA).
		Northeast Illinois Regional Commuter Railroad Corporation (Metra/NIRCRC).
		Northern Indiana Commuter Transportation District (NICTD).
		PACE Suburban Bus Company.
MA	Boston Area	Massachusetts Bay Transportation Authority (MBTA).

State	Urban area	Systems
NY/NJ/CT	New York City/Northern New Jersey Area (New York City and Jersey City/Newark urban Areas).	Connecticut Department of Transportation (CDOT). Connecticut Transit (Hartford Division and New Haven Divisions of CTTransit). Metropolitan Transportation Authority (All Agencies). New Jersey Transit Corp. (NJT). New York City Department of Transportation. Port Authority Trans-Hudson Corporation (Port Authority of New York and New Jersey) (PANYNJ) (excluding ferry). Westchester County Department of Transportation Bee-Line System (The Bee-Line System).
PA/NJ	Philadelphia Area	Delaware River Port Authority (DRPA)—Port Authority Transit Corporation (PATCO). Delaware Transit Corporation (DTC). New Jersey Transit Corp. (NJT) (covered under NY). Pennsylvania Department of Transportation. Southeastern Pennsylvania Transportation Authority (SEPTA).

Appendix B to Part 1582—Security-Sensitive Job Functions For Public Transportation and Passenger Railroads

This table identifies security-sensitive job functions for owner/operators regulated under this part. All employees performing security-sensitive functions are ''security-sensitive employees'' for purposes of this rule and must be trained.

Categories	Security-sensitive job functions for public transportation and passenger railroads (PTPR)
A. Operating a vehicle	1. Employees who— a. Operate or control the movements of trains, other rail vehicles, or transit buses. b. Act as train conductor, trainman, brakeman, or utility employee or performs acceptance inspections, couples and uncouples rail cars, applies handbrakes, or similar functions. 2. Employees covered under the Federal hours of service laws as ''train employees.'' *See* 49 U.S.C. 21101(5) and 21103.
B. Inspecting and maintaining vehicles	Employees who— 1. Perform activities related to the diagnosis, inspection, maintenance, adjustment, repair, or overhaul of electrical or mechanical equipment relating to vehicles, including functions performed by mechanics and automotive technicians. 2. Provide cleaning services to vehicles owned, operated, or controlled by an owner/operator regulated under this subchapter.
C. Inspecting or maintaining building or transportation infrastructure	Employees who— 1. Maintain, install, or inspect communication systems and signal equipment related to the delivery of transportation services. 2. Maintain, install, or inspect track and structures, including, but not limited to, bridges, trestles, and tunnels. 3. Provide cleaning services to stations and terminals owned, operated, or controlled by an owner/operator regulated under this subchapter that are accessible to the general public or passengers. 4. Provide maintenance services to stations, terminals, yards, tunnels, bridges, and operation control centers owned, operated, or controlled by an owner/operator regulated under this subchapter. 5. Employees covered under the Federal hours of service laws as ''signal employees.'' *See* 49 U.S.C. 21101(4) and 21104.
D. Controlling dispatch or movement of a vehicle	Employees who— 1. Dispatch, report, transport, receive or deliver orders pertaining to specific vehicles, coordination of transportation schedules, tracking of vehicles and equipment. 2. Manage day-to-day management delivery of transportation services and the prevention of, response to, and redress of service disruptions. 3. Supervise the activities of train crews, car movements, and switching operations in a yard or terminal. 4. Dispatch, direct, or control the movement of trains or buses. 5. Operate or supervise the operations of moveable bridges. 6. Employees covered under the Federal hours of service laws as ''dispatching service employees.'' *See* 49 U.S.C. 21101(2) and 21105.
E. Providing security of the owner/operator's equipment and property ...	Employees who— 1. Provide for the security of PTPR equipment and property, including acting as a police officer.

Categories	Security-sensitive job functions for public transportation and passenger railroads (PTPR)
	2. Patrol and inspect property of an owner/operator regulated under this subchapter to protect the property, personnel, passengers and/or cargo.
F. Loading or unloading cargo or baggage	Employees who load, or oversee loading of, property tendered by or on behalf of a passenger on or off of a portion of a train that will be inaccessible to the passenger while the train is in operation.
G. Interacting with travelling public (on board a vehicle or within a transportation facility).	Employees who provide services to passengers on-board a train or bus, including collecting tickets or cash for fares, providing information, and other similar services. Including: 1. On-board food or beverage employees. 2. Functions on behalf of an owner/operator regulated under this subchapter that require regular interaction with travelling public within a transportation facility, such as ticket agents.
H. Complying with security programs or measures, including those required by Federal law.	1. Employees who serve as security coordinators designated in § 1570.201 of this subchapter, as well as any designated alternates or secondary security coordinators. 2. Employees who— a. Conduct training and testing of employees when the training or testing is required by TSA's security regulations. b. Manage or direct implementation of security plan requirements.

■ 13. Add part 1584 to read as follows:

PART 1584—HIGHWAY AND MOTOR CARRIER SECURITY

Subpart A—General

Subpart B—Security Programs

Authority: 49 U.S.C. 114; Pub. L. 110–53 (121 Stat. 266, Aug. 3, 2007) secs. 1501 (6 U.S.C. 1151), 1531 (6 U.S.C. 1181), and 1534 (6 U.S.C. 1184).

Subpart A—General

§ 1584.1 Scope.

This part includes requirements for persons providing transportation by an over-the-road bus (OTRB). Specific sections in this part provide detailed requirements.

§ 1584.3 Terms used in this part.

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-sensitive employee means an employee whose responsibilities for the owner/operator include one or more of the security-sensitive job functions identified in Appendix B to this part where the security-sensitive function is performed in the United States or in direct support of the common carriage of persons or property between a place in the United States and any place outside of the United States.

Subpart B—Security Programs

§ 1584.101 Applicability.

The requirements of this subpart apply to each OTRB owner/operator providing fixed-route service that originates, travels through, or ends in a geographic location identified in appendix A to this part.

§ 1584.103 [Reserved]

§ 1584.105 [Reserved]

§ 1584.107 [Reserved]

§ 1584.109 [Reserved]

§ 1584.111 [Reserved]

§ 1584.113 Security training program general requirements.

(a) *Security training program required.* Each owner/operator identified in § 1584.101 of this part is required to adopt and carry out a security training program under this subpart.

(b) *General requirements.* The security training program must include the following information:

(1) Name of owner/operator.

(2) Name, title, telephone number, and email address of the primary individual to be contacted with regard to review of the security training program.

(3) Number, by specific job function category identified in Appendix B to this part, of security-sensitive employees trained or to be trained.

(4) Implementation schedule that identifies a specific date by which initial and recurrent security training required by § 1570.111 of this subchapter will be completed.

(5) Location where training program records will be maintained.

(6) Curriculum or lesson plan, including learning objectives and method of delivery (such as instructor-led or computer-based training) for each course used to meet the requirements of § 1584.115 of this part. TSA may request additional information regarding the curriculum during the review and approval process. If recurrent training under § 1570.111 of this subchapter is not the same as initial training, a curriculum or lesson plan for the recurrent training will need to be submitted and approved by TSA.

(7) Plan for ensuring supervision of untrained security-sensitive employees performing functions identified in Appendix B to this part.

(8) Plan for notifying employees of changes to security measures that could change information provided in previously provided training.

(9) Method(s) for evaluating the effectiveness of the security training program in each area required by § 1584.115 of this part.

(c) *Relation to other training.* (1) Training conducted by owner/operators to comply other requirements or standards may be combined with and used to satisfy elements of the training requirements in this subpart.

(2) If the owner/operator submits a security training program that relies on pre-existing or previous training materials to meet the requirements of subpart B, the program submitted for approval must include an index, organized in the same sequence as the requirements in this subpart.

(d) *Submission and Implementation.* The owner/operator must submit and implement the security training program in accordance with the schedules identified in §§ 1570.109 and 1570.111 of this subchapter.

§ 1584.115 Security training and knowledge for security-sensitive employees.

(a) *Training required for security-sensitive employees.* No owner/operator required to have a security training program under § 1584.101 of this part may use a security-sensitive employee to perform a function identified in Appendix B to this part unless that individual has received training as part of a security training program approved by TSA under 49 CFR part 1570, subpart B, or is under the direct supervision of an employee who has received the training required by this section as applicable to that security-sensitive function.

(b) *Limits on use of untrained employees.* Notwithstanding paragraph (a) of this section, a security-sensitive employee may not perform a security-sensitive function for more than sixty (60) calendar days without receiving security training.

(c) *Prepare.* Each owner/operator must ensure that each of its security-sensitive employees with position- or function-specific responsibilities under the owner/operator's security program have knowledge of how to fulfill those responsibilities in the event of a security threat, breach, or incident to ensure—

(1) Employees with responsibility for transportation security equipment and systems are aware of their responsibilities and can verify the equipment and systems are operating and properly maintained; and

(2) Employees with other duties and responsibilities under the company's security plans and/or programs, including those required by Federal law, know their assignments and the steps or resources needed to fulfill them.

(d) *Observe.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of the observational skills necessary to recognize—

(1) Suspicious and/or dangerous items (such as substances, packages, or conditions (for example, characteristics of an IED and signs of equipment tampering or sabotage);

(2) Combinations of actions and individual behaviors that appear suspicious and/or dangerous, inappropriate, inconsistent, or out of the ordinary for the employee's work environment, which could indicate a threat to transportation security; and

(3) How a terrorist or someone with malicious intent may attempt to gain sensitive information or take advantage of vulnerabilities.

(e) *Assess.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge necessary to—

(1) Determine whether the item, individual, behavior, or situation requires a response as a potential terrorist threat based on the respective transportation environment; and

(2) Identify appropriate responses based on observations and context.

(f) *Respond.* Each owner/operator must ensure that each of its security-sensitive employees has knowledge of how to—

(1) Appropriately report a security threat, including knowing how and when to report internally to other employees, supervisors, or management, and externally to local, state, or Federal agencies according to the owner/operator's security procedures or other relevant plans;

(2) Interact with the public and first responders at the scene of the threat or incident, including communication with passengers on evacuation and any specific procedures for individuals with disabilities and the elderly; and

(3) Use any applicable self-defense devices or other protective equipment provided to employees by the owner/operator.

Appendix A to Part 1584—Urban Area Determinations for Over-the-Road Buses

State	Urban area	Geographic areas
CA	Anaheim/Los Angeles/Long Beach/Santa Ana Areas.	Los Angeles and Orange Counties.
	San Diego Area	San Diego County.
	San Francisco Bay Area	Alameda, Contra Costa, Marin, San Francisco, and San Mateo Counties.
DC (VA, MD, and WV).	National Capital Region	District of Columbia; Counties of Calvert, Charles, Frederick, Montgomery, and Prince George's, MD; Counties of Arlington, Clarke, Fairfax, Fauquier, Loudoun, Prince William, Spotsylvania, Stafford, and Warren County, VA; Cities of Alexandria, Fairfax, Falls Church, Fredericksburg, Manassas, and Manassas Park City, VA; Jefferson County, WV.
IL/IN	Chicago Area	Counties of Cook, DeKalb, DuPage, Grundy, Kane, Kendall, Lake, McHenry, and Will, IL; Counties of Jasper, Lake, Newton, and Porter, IN; Kenosha County, WI.
MA	Boston Area	Counties of Essex, Norfolk, Plymouth, Suffolk, Middlesex, MA; Counties of Rockingham and Strafford, NH.
NY (NJ and PA).	New York City/Jersey City/Newark Area.	Counties of Bronx, Kings, Nassau, New York, Putnam, Queens, Richmond, Rockland, Suffolk, and Westchester, NY; Counties of Bergen, Essex, Hudson, Hunterdon, Ocean, Middlesex, Monmouth, Morris, Passaic, Somerset, Sussex, and Union, NJ; Pike County, PA.
PA (DE and NJ).	Philadelphia Area/Southern New Jersey Area.	Counties of Burlington, Camden, and Gloucester, NJ; Counties of Bucks, Chester, Delaware, Montgomery, and Philadelphia, PA; New Castle County, DE; Cecil County, MD; Salem County, NJ.
TX	Dallas Fort Worth/Arlington Area	Collin, Dallas, Delta, Denton, Ellis, Hunt, Kaufman, Rockwall, Johnson, Parker, Tarrant, and Wise Counties, TX.
	Houston Area	Austin, Brazoria, Chambers, Fort Bend, Galveston, Harris, Liberty, Montgomery, San Jacinto, and Waller Counties, TX.

Appendix B to Part 1584—Security-Sensitive Job Functions for Over-the-Road Buses

This table identifies security-sensitive job functions for owner/operators regulated under this part. All employees performing security-sensitive functions are ''security-sensitive employees'' for purposes of this rule and must be trained.

Categories	Security-sensitive job functions for over-the-road buses
A. Operating a vehicle	Employees who have a CDL and operate an OTRB.
B. Inspecting and maintaining vehicles	Employees who— 1. Perform activities related to the diagnosis, inspection, maintenance, adjustment, repair, or overhaul of electrical or mechanical equipment relating to vehicles, including functions performed by mechanics and automotive technicians. 2. Does not include cleaning or janitorial activities.
C. Inspecting or maintaining building or transportation infrastructure.	Employees who— 1. Provide cleaning services to areas of facilities owned, operated, or controlled by an owner/operator regulated under this subchapter that are accessible to the general public or passengers. 2. Provide cleaning services to vehicles owned, operated, or controlled by an owner/operator regulated under this part (does not include vehicle maintenance). 3. Provide general building maintenance services to buildings owned, operated, or controlled by an owner/operator regulated under this part.
D. Controlling dispatch or movement of a vehicle.	Employees who— 1. Dispatch, report, transport, receive or deliver orders pertaining to specific vehicles, coordination of transportation schedules, tracking of vehicles and equipment. 2. Manage day-to-day delivery of transportation services and the prevention of, response to, and redress of disruptions to these services. 3. Perform tasks requiring access to or knowledge of specific route information.
E. Providing security of the owner/operator's equipment and property.	Employees who patrol and inspect property of an owner/operator regulated under this part to protect the property, personnel, passengers and/or cargo.
F. Loading or unloading cargo or baggage	Employees who load, or oversee loading of, property tendered by or on behalf of a passenger on or off of a portion of a bus that will be inaccessible to the passenger while the vehicle is in operation.
G. Interacting with travelling public (on board a vehicle or within a transportation facility).	Employees who— 1. Provide services to passengers on-board a bus, including collecting tickets or cash for fares, providing information, and other similar services. 2. Includes food or beverage employees, tour guides, and functions on behalf of an owner/operator regulated under this part that require regular interaction with travelling public within a transportation facility, such as ticket agents.
H. Complying with security programs or measures, including those required by Federal law.	1. Employees who serve as security coordinators designated in § 1570.201 of this subchapter, as well as any designated alternates or secondary security coordinators. 2. Employees who— a. Conduct training and testing of employees when the training or testing is required by TSA's security regulations. b. Manage or direct implementation of security plan requirements.

Dated: February 28, 2020.

David P. Pekoske,

Administrator.

[FR Doc. 2020–05126 Filed 3–20–20; 8:45 am]

BILLING CODE 9110–05–P