[9110-05-P]

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Chapter **XII**

[Docket No. TSA-2016-0002]

RIN 1652-AA56

Surface Transportation Vulnerability Assessments and Security Plans (VASP)

AGENCY: Transportation Security Administration, DHS.

ACTION: Advance notice of proposed rulemaking (ANPRM).

SUMMARY: The Transportation Security Administration (TSA) is issuing this ANPRM to request public comments on several topics relevant to the development of surface transportation vulnerability assessment and security plan regulations mandated by the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act). Based on its regular interaction with stakeholders, TSA assumes many higher-risk railroads (freight and passenger), public transportation agencies, and over-the-road buses (OTRBs) have implemented security programs with security measures similar to those identified by the 9/11 Act's regulatory requirements. In general, TSA is requesting information on three types of issues. First, existing practices, standards, tools, or other resources used or available for conducting vulnerability assessments and developing security plans. Second, information on existing security measures, including whether implemented voluntarily or in response to other regulatory requirements, and the potential impact of additional requirements on operations. Third, information on the scope/cost of current security systems and other measures used to provide security and mitigate vulnerabilities. This

information is necessary for TSA to establish the current baseline, estimate cost of implementing the statutory mandate, and develop appropriate performance standards.

While TSA will review and consider all comments submitted, TSA invites responses to a number of specific questions posed in the ANPRM. See the Comments Invited section under SUPPLEMENTARY INFORMATION that follows.

DATES: Submit comments by [Insert date 60 days after date of publication in the Federal Register].

ADDRESSES: You may submit comments, identified by the TSA docket number to this rulemaking, to the Federal Docket Management System (FDMS), a government-wide, electronic docket management system, using any one of the following methods:

Electronically: You may submit comments through the Federal eRulemaking portal at http://www.regulations.gov. Follow the online instructions for submitting comments.

Mail, In Person, or Fax: Address, hand-deliver, or fax your written comments to the Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE, West Building Ground Floor, Room W12-140, Washington, DC 20590-0001; fax (202) 493-2251. The Department of Transportation (DOT), which maintains and processes TSA's official regulatory dockets, will scan the submission and post it to FDMS.

See SUPPLEMENTARY INFORMATION for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: Harry Schultz (TSA Office of Security Policy and Industry Engagement) or Traci Klemm (TSA Office of the Chief Counsel) at telephone (571) 227-3531 or e-mail to VASPPOLICY@tsa.dhs.gov.

SUPPLEMENTARY INFORMATION:

Comments Invited

TSA invites interested persons to participate in this rulemaking by submitting written comments, data, or views. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking action. See ADDRESSES above for information on where to submit comments.

With each comment, please identify the docket number at the beginning of your comments. You may submit comments and material electronically, in person, by mail, or fax as provided under ADDRESSES, but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you would like TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. TSA will stamp the date on the postcard and mail it to you.

TSA will file all comments to our docket address, as well as items sent to the address or email under FOR FURTHER INFORMATION CONTACT, in the public docket, except for comments containing confidential information and sensitive security information (SSI)[1]. Should you wish your personally identifiable information redacted

[1] "Sensitive Security Information" or "SSI" is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets

prior to filing in the docket, please so state. TSA will consider all comments that are in the docket on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Specific Questions

In general, TSA seeks comments on the broad areas outlined within this ANPRM and approaches TSA can take to integrate existing requirements and voluntarily initiated programs to enhance security as intended by the statutory requirements this rulemaking will fulfill. TSA also seeks comments on how this rulemaking could be implemented to meet the requirements of the law in a manner that maximizes benefits without imposing excessive, unjustified, or unnecessary costs.

Specific questions are included in this ANPRM immediately following the discussion of the relevant issues. TSA asks that commenters provide as much information as possible. In some areas, TSA requests very specific information. Whenever possible, please provide citations and copies of any relevant studies or reports on which you rely, as well as any additional data which supports your comment. It is also helpful to explain the basis and reasoning underlying your comment.

TSA appreciates any information provided. While complete answers are preferable, TSA recognizes that providing detailed comments on every question could be burdensome and will consider all comments, regardless of whether the response is complete. Each commenting party should include the identifying number of the specific question(s) to which it is responding. To assist commenters, a fillable template with all of the questions

---

or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

in sequential order is included in the docket. Commenters can download the template, complete it, and then upload it to the docket or submit a hard copy as directed under ADDRESSES.

TSA will use comments to make decisions regarding the content and direction of the notice of proposed rulemaking (NPRM). TSA also requests additional comments and information not addressed by these questions that would promote an understanding of the implications of imposing a VASP regulatory requirement. TSA does not expect that every commenter will be able to answer every question. Please respond to those questions you feel able to answer or that address your particular issue.

TSA encourages responses from all interested entities, not just the transportation sectors to which this rulemaking would apply. Each comment filed by a party, other than public transportation agencies, railroads, or OTRB companies, or their representatives, should explain the commenter's interest in this rulemaking and how their comments may assist in TSA's development of the regulation.

Handling of Confidential or Proprietary Information and SSI Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in the FOR FURTHER INFORMATION CONTACT section.

TSA will not place comments containing SSI in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold documents containing SSI, confidential business information, or trade secrets in a separate file to which the public does not have access, and place a note in the public docket explaining that commenters have submitted such documents. TSA may include a redacted version of the comment in the public docket. If an individual requests to examine or copy information that is not in the public docket, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the Department of Homeland Security's (DHS') FOIA regulation found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments in any of our dockets by the name of the individual who submitted the comment (or signed the comment, if an association, business, labor union, etc., submitted the comment). You may review the applicable Privacy Act Statement published in the Federal Register on April 11, 2000 (65 FR 19477), and modified on January 17, 2008 (73 FR 3316).

You may review TSA's electronic public docket on the Internet at http://www.regulations.gov. In addition, DOT's Docket Management Facility provides a physical facility, staff, equipment, and assistance to the public. To obtain assistance or to review comments in TSA's public docket, you may visit this facility between 9:00 a.m. and 5:00 p.m., Monday through Friday, excluding legal holidays, or call (202) 366-9826. This docket operations facility is located in the West Building Ground Floor, Room W12-140 at 1200 New Jersey Avenue, SE, Washington, DC 20590.

Availability of Rulemaking Document

You can get an electronic copy using the Internet by—

(1) Searching the electronic FDMS web page at http://www.regulations.gov; or

(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.

Abbreviations and Terms Used in This Document

17 SAIs - 17 Security and Emergency Preparedness Action Items for Transit Agencies

AAR - Association of American Railroads

AMTRAK - National Railroad Passenger Corporation

ANPRM - Advance Notice of Proposed Rulemaking

APTA -American Public Transportation Association

BASE - Baseline Assessment for Security Enhancement

CSRs - Corporate Security Reviews

DOT - Department of Transportation

DHS - Department of Homeland Security

EXIS - Exercise Information System

FEMA - Federal Emergency Management Agency

FMCSA - Federal Motor Carrier Safety Administration

FRA - Federal Railroad Administration

FTA - Federal Transit Administration

HMR - Hazardous Materials Regulations

HSA - Homeland Security Act of 2002

HSAS - Homeland Security Advisory System

HSEEP - Homeland Security Exercise and Evaluation Program

HTUA - High-Threat Urban Area

I-STEP - Intermodal Security Training and Exercise Program

NCIPP - National Critical Infrastructure Prioritization Program

NPRM - Notice of Proposed Rulemaking

NTAS - National Terrorism Advisory System

NY MTA - New York Metropolitan Transportation Authority

OMB - Office of Management and Budget

OTRB - Over-the-Road Bus

OAs - Oversight Agencies

PHMSA - Pipeline and Hazardous Materials Safety Administration

PPD - Presidential Policy Directive

PRA - Paperwork Reduction Act of 1995

PTPR - Public Transportation and Passenger Railroads

RSSM - Rail Security-Sensitive Materials

RTAs - Rail Transit Agencies

SMARToolbox - Security Measures and Resources Toolbox

SSI - Sensitive Security Information

SSO - State Safety Oversight

STB - Surface Transportation Board

TSA - Transportation Security Administration

TSGP - Transit Security Grant Program

T-START - Transportation Security Template and Assessment Review Toolkit

TWIC - Transportation Worker Identification Credential

UASI - Urban Area Security Initiative

VASP - Vulnerability Assessments and Security Plans

Table of Contents

VII. Accountable Executive

IX. Considerations for Small Owner/Operators

X. Estimating the Benefits and Costs of Requirements

XI. Next Steps and Public Participation

I. Introduction

This ANPRM is part of a series of rulemakings applicable to public transportation and passenger railroads (PTPR) systems, freight railroads, and OTRBs to comply with requirements of the 9/11 Act.[2] The 9/11 Act requires TSA to promulgate regulations involving: (1) security training of frontline employees,[3] (2) vulnerability assessments and security plans,[4] and (3) employee vetting.[5]

This ANPRM is limited to the requirements for VASP regulations. Through this ANPRM, TSA is seeking comments on: (1) requirements for vulnerability assessments of security systems and operations and critical assets/infrastructure, (2) requirements for security plans, and (3) resources or other required programs that TSA should consider as relevant for meeting these requirements. Knowledgeable and constructive input from railroads, public transportation agencies, OTRB operators, their representative associations, labor unions, state and local governments, and the general public who rely on these systems is critical for developing a regulation with the proper balance between costs and benefits.

By imposing VASP requirements on higher-risk railroads, public transportation agencies, and OTRBs, this rulemaking should establish a uniform base of vulnerability

[2] Pub. L. 110-53, 121 Stat. 266 (Aug. 3, 2007).
[3] Id. secs. 1408, 1517, and 1534. For a discussion regarding the applicability of the 9/11 Act to these proposed rules, see Section II of this ANPRM.
[4] 9/11 Act secs. 1405, 1512, and 1531. See also Section II of this ANPRM.
[5] 9/11 Act secs. 1411, 1520, and 1531(e)(2). See also Section II of this ANPRM.

assessments and security plans for security systems and operations, as well as critical assets and/or infrastructure that these owner/operators may own or control.

TSA believes the VASP regulations should consider current voluntarily implemented security measures and operational issues in establishing performance standards for compliance. To that end, TSA is seeking specific information to assist in developing effective regulatory policies, resources for implementation, and valid cost estimates. To provide context for the questions, this ANPRM is organized to include requests for comment immediately following discussions of the relevant issues.

TSA is requesting public comment and data to assist in identifying the current baseline in order to determine the incremental cost of compliance with the assessment and planning elements required by the 9/11 Act. In general, TSA is particularly interested in data from surface transportation owner/operators who currently have security plans specifically based on a vulnerability or similar assessment. For example, TSA needs data on the cost of conducting an assessment (if not conducted by TSA), cost of developing a security plan, and the types and cost of risk-reduction or mitigation measures. While TSA has gathered significant information in these areas as part of its ongoing rulemaking efforts, there are some areas where it would be helpful to validate cost elements and ensure our understanding of the existing baseline is current. The requests for comment seek information to close these information gaps.

As discussed below, TSA is concerned about the impact of this regulation based on the diversity of surface transportation owner/operators, which could include large (national) companies, publicly owned systems, and small businesses. While not required, TSA asks commenters to include information regarding the nature and size of the

business. Information on the nature of the business operation of the person commenting will help TSA better understand and analyze the information provided. Failure to include this specific information will not preclude the agency's consideration of the information submitted.

II. Background

A. Surface Transportation

The surface transportation rules required by the 9/11 Act must address a decentralized, diffuse, complex, and evolving terrorist threat in the context of an inherently open and diverse transportation system. The U.S. surface transportation network is immense, consisting of public transportation systems, passenger and freight railroads, highways, motor carrier operators, pipelines, and maritime facilities. The New York Metropolitan Transportation Authority (NY MTA) alone transports over 11 million passengers daily and represents just one of the more than 6,800 U.S. public transit agencies for which TSA has oversight, ranging from very small bus-only systems in rural areas to very large multi-modal systems in urban areas like the NY MTA. More than 500 individual freight railroads operate on nearly 140 thousand miles of track carrying essential goods. Eight million large capacity commercial trucks and almost 4 thousand commercial bus companies travel on the 4 million miles of roadway in the United States and on more than 600 thousand highway bridges and through 350 tunnels greater than 300 feet in length. Surface transportation operators carry approximately 750 million intercity bus passengers and 10 billion passenger trips on public transportation each year. Securing such diverse surface transportation systems in a society that depends upon the

free movement of people and commerce is a complex undertaking that requires extensive collaboration with surface transportation operators.

Unlike the aviation mode of transportation, direct responsibility to secure surface transportation systems falls primarily on the system owners and operators. In further contrast to aviation, surface transportation systems are, by nature, open systems. Surface transportation systems can be national and privately held companies, public transportation systems owned and operated by the government, or a family-owned business with two buses. Regardless of the size of the business, surface transportation owner/operators are in the best position to know their facilities and their operational challenges. As a whole, these owner/operators have spent billions of dollars of their own funds to secure critical infrastructure, provide uniformed law enforcement and specialty security teams, and conduct operational activities and deterrence efforts.

Security and emergency response planning is not new to surface transportation owner/operators; they have been working under DOT[6] and DHS[7] regulations. Although DOT's regulations relate primarily to safety, many safety activities and programs also benefit security and help to reduce risk. In the surface environment, TSA has built upon these standards to improve security programs with minimal regulations.

---

[6]For example, the Pipeline and Hazardous Materials Safety Administration regulates the transportation of hazardous materials in commerce, including requirements for safety and security training and for security planning (49 CFR parts 171-180); the Federal Railroad Administration regulates passenger train emergency preparedness (49 CFR parts 200-299); and the Federal Transit Administration requires system safety programs for rail transit agencies (49 CFR part 659).

[7]For example, the Transportation Worker Identification Credential (TWIC) program is a TSA and U.S. Coast Guard initiative in the United States. For more information, see https://www.tsa.gov/for-industry/twic. A TWIC is required for workers who need access to secure areas of the nation's maritime facilities and vessels. TSA conducts a security threat assessment (background check) to determine a person's eligibility and issues the credential. U.S. citizens and immigrants in certain immigration categories may apply for the credential. Most mariners licensed by the U.S. Coast Guard also require a credential. See 49 CFR part 1572. The National Protection and Programs Directorate of DHS regulates the security of certain high-risk chemical facilities in the United States. See 6 CFR part 27.

B. TSA's Role and Responsibility

TSA is responsible for assessing security risks for any mode of transportation, developing appropriate security measures for dealing with those risks, and ensuring implementation of those measures.[8] Assessments include analysis of intelligence information and on-site reviews of transportation systems and operations. TSA works collaboratively with its surface stakeholders to enhance information sharing and develop security measures and best practices appropriate for the operational environment. DHS provides funding to support information sharing and implementation of security measures. This funding supports information sharing and analysis centers (ISACs) that facilitate threat warning and incident reporting for railroads, public transportation systems, and over-the-road buses. In addition, TSA works with DHS to develop and implement a risk-based determination for allocation of Federal grant funds. Eligible surface transportation owner/operators can supplement their own investment in security, using this funding to identify and mitigate operational vulnerabilities.

TSA can also ensure implementation through promulgation of regulations.[9] For example, the Rail Transportation Security regulation (published in 2008 and codified at 49 CFR part 1580) requires all rail systems (freight, passenger, and public transportation)

[8] See 49 U.S.C. 114(d) and (f), codifying provisions of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, 115 Stat. 597 (Nov. 19, 2001). ATSA created TSA and made it the primary federal agency responsible to enhance security for all modes of transportation. Section 403(2) of the Homeland Security Act of 2002 (HSA), Pub. L. 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 related to TSA, to the Secretary of Homeland Security. Pursuant to DHS, "Delegation to the Administrator of the Transportation Security Administration," Delegation Number 7060.2 (Nov. 5, 2003), 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 that in sec. 403(2) of the HSA.

[9] 49 U.S.C. 114(l)(1).

to appoint rail security coordinators[10] and report significant security concerns to TSA through the Transportation Security Operations Center (located at the "Freedom Center").[11] In addition, freight railroads are required to report (upon request by TSA) the location and shipping information for rail cars containing certain hazardous materials and provide "chain of custody" to ensure security of those materials when transported through high-risk areas.[12]

C. The 9/11 Act

The 9/11 Act includes numerous mandates related to surface transportation security. These requirements include development of security strategies, reporting on implementation, information sharing, civil penalties, Visible Intermodal Prevention and Response teams, security assessments, grant programs for security enhancements, a national security exercise program, background check programs, protection for employees reporting security violations, public outreach campaigns, and studies on particular hazards and threats.[13]

As previously noted, the 9/11 Act also mandates that TSA require VASP for higher-risk public transportation agencies, railroads, and OTRBs; security training of their frontline employees; and, employee background checks.[14] TSA is addressing these

[10] 49 CFR 1580.101 and 1580.201.
[11] 49 CFR 1580.105 and 1580.203.
[12] 49 CFR 1580.107.
[13] See 9/11 Act, at Title XII (Transportation Security Planning and Information Sharing), Title XIII (Transportation Security Enhancements), Title XIV (Public Transportation Security), and Title XV (Surface Transportation Security).
[14] See 9/11 Act secs. 1405, 1512, and 1531 for VASP requirements; secs. 1408, 1517, and 1534 for employee security training requirements; and secs. 1411 and 1520 for employee vetting requirements. The statutory mandates for VASP in secs. 1512, and 1531 also include a requirement to conduct security threat assessments of security coordinators.

requirements in three separate, but related, rulemakings.[15] The docket for this ANPRM includes a table aligning the statutory provisions for VASP across the three modes (public transportation, railroads, and OTRBs).

D. Applicability

For purposes of this ANPRM, TSA is limiting the scope of its request for comments related to applicability. As previously noted, the VASP rulemaking is part of a series of rulemakings to implement requirements of the 9/11 Act. As the first of these rulemakings published by TSA, the Security Training NPRM provides the general structure, including proposed applicability and the framework for a regulatory program. TSA intends for the applicability proposed in the Security Training NPRM to apply generally to the three related rulemakings.[16] In other words, the higher-risk PTPR, freight railroad, and OTRB owner/operators required to have a security-training program (surface owner/operators) would also be required to conduct vulnerability assessments, implement security plans, and implement requirements for employee vetting (security threat assessments).

Consistent with the proposed applicability for the Security Training NPRM, TSA assumes the VASP requirements would apply to--

[15] TSA published an NPRM to implement requirements related to employee security training, titled "Security Training Programs for Surface Transportation Employees," published elsewhere in this issue of the Federal Register. TSA will address requirements for employee vetting in a separate NPRM. See Fall 2016 Unified Agenda, RIN 1652-AA69.

[16] The Security Training NPRM incorporates all of requirements in current 49 CFR part 1580. The rail operations subject to the requirements in current part 1580 is broader than the proposed applicability for rail operations in the Security Training NPRM. To the extent an owner/operator must comply with requirements in current part 1580, applicability proposed in the Security Training NPRM would not affect that obligation. For example, if a railroad is required to have a security coordinator under current part 1580, but is not within the scope of proposed applicability for security training, they must still have a security coordinator. TSA anticipates capturing this additional security coordinator population in the related rulemaking for vetting requirements, consistent with the 9/11 Act's requirement to conduct security threat assessments of all security coordinators. See 9/11 Act secs. 1512(e)(2) and 1531(e)(2).

- Class 1 railroads (as assigned by regulations of the Surface Transportation Board (STB) (49 CFR part 1201; General Instructions 1-1);
- Railroads transporting rail security-sensitive materials (RSSM)[17] in a high-threat urban area (HTUA);
- Railroads hosting higher-risk rail operations (including freight railroads and the intercity or commuter systems);
- PTPR systems identified as higher-risk operating in one of the following eight regions (geographically consistent with designations under the Urban Area Security Initiative (UASI)): San Francisco Bay area, Los Angeles/Long Beach and Anaheim/Santa Ana areas, National Capital Region and Baltimore areas, Atlanta area, Chicago area, Boston area, New York City and Jersey City/Newark areas, and Philadelphia area;
- Amtrak (the Security Training NPRM includes a list of systems); and
- OTRB owner/operators providing fixed-route service to, through, or from one of the following areas (geographically consistent with designations under the UASI): Anaheim/Los Angeles/Long Beach/Santa Ana areas, San Diego area, San Francisco Bay area, National Capital Region, Boston area, New York City/Jersey City/Newark area, Philadelphia area/Southern New Jersey area, Dallas/Fort Worth/Arlington area, Chicago area, and Houston area.

As TSA has included a full discussion of the proposed and alternative applicability options in the Security Training NPRM, as well as an opportunity to comment, that discussion is not duplicated as part of this ANPRM. Later in this

[17] See definition in proposed 49 CFR 1580.3 of the Security Training NPRM, which is consistent with the definition in current 49 CFR 1580.100(b).

ANPRM, however, a specific request for comments is included for the impact on small businesses. TSA will consider all comments received on this ANPRM.

III. Rulemaking Context

The baseline of security for surface transportation has been substantially enhanced since the 9/11 Act was enacted through programs (including some required by the 9/11 Act), and the cooperative and collaborative relationship between TSA and the surface transportation industry. These relationships have led to enhanced security through development of best practices, sharing of information (both reporting of security-related incidents by the industry, intelligence sharing by the government, and other efforts such as the ISACs), and security programs and measures to strengthen and enhance the security of surface transportation networks.

The VASP regulations will be part of this broad and sustained effort to develop and maintain an enhanced security baseline for surface transportation as well as strengthening the security of nationally significant critical assets. Understanding the scope of these efforts is essential to this rulemaking as the 9/11 Act specifically authorizes TSA to recognize existing procedures, protocols, and standards that can be used to meet all or part of the regulatory requirements for assessments and planning.[18] Additional information on a few of these programs is provided below.

A. Grant Programs

The 9/11 Act authorized funding for surface security enhancements specifically for PTPR, freight railroads, and OTRB owner/operators.[19] To the extent funds are appropriated for this purpose, TSA provides the Federal Emergency Management

[18] See 9/11 Act secs. 1405(i), 1512(j), and 1531(i).
[19] See 9/11 Act secs. 1406(a)(2) (public transportation security assistance), 1513(a)(2) (railroads), 1514(b) (Amtrak), and 1532(f)(1) (OTRBs).

Agency (FEMA) with subject matter expertise, assisting in the development of risk determinations, review of investment justifications, and other aspects of the surface transportation security grant programs. These grants support surface transportation risk-reduction or mitigation measures by applying Federal funding to critical security projects. Between fiscal years (FYs) 2006 and 2016, DHS awarded more than $2.4 billion in transportation security grant funding to freight railroad carriers and operators, OTRB operators, the trucking community, and public mass transit owners and operators, including Amtrak, and their dedicated law enforcement providers. Congress appropriated $100 million in FY 2016, from which DHS awarded $87 million for mass transit, $10 million for passenger rail, and $3 million for motor coach security grants.

TSA assumes surface transportation owner/operators will incorporate security measures and other security enhancements funded by these grant programs into security programs complying with the regulatory requirements mandated by the 9/11 Act. This assumption recognizes requirements in the authorizing statutes for these grant programs, which all prioritized funding for meeting 9/11 Act requirements for security training, assessments, and planning.

B. Intermodal Security Training and Exercise Program

The 9/11 Act also required development of a security exercise program to "assess[] and improv[e] the capabilities" of surface modes "to prevent, prepare for, mitigate against, respond to, and recover from acts of terrorism."[20] TSA implemented this requirement through the Intermodal Security Training and Exercise Program (I-STEP). I-STEP brings public and private sector partners together to exercise, train, share

[20] See 9/11 Act secs. 1407, 1516 and 1533. See also sec. 114 of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Pub. L. 109-347, 120 Stat. 1884, 1896-97 (Oct. 13, 2006).

information, and address transportation security issues to protect travelers, commerce, and infrastructure. Through the program, TSA facilitates modal and intermodal exercises and workshops throughout the country. The program also provides training support to help modal operators meet their training objectives. The Exercise Information System (EXIS) is an online tool developed by TSA, which leverages the concept of I-STEP in support of all operators, but particularly those operators that may be less competitive for I-STEP exercises because they are lower risk systems.

C. Department of Transportation Regulations

1. Hazardous Material Regulations

DOT modes also have regulatory programs that may be relevant to meeting VASP requirements. For example, every freight railroad transporting at least one of the hazardous materials that trigger applicability under 49 CFR part 172 (known as the Hazardous Materials Regulations (HMR)) is required to have and adhere to a security plan. While the security plan requirements of the HMR may not be identical to the requirements in the 9/11 Act, TSA anticipates that freight railroad owner/operators may be able to use plans developed and implemented under the HMR to satisfy a portion of TSA's VASP regulations.

2. Transit Safety and Security

The Federal Transit Administration (FTA) has responsibility for managing State oversight for rail transit agencies (RTAs). Under 49 CFR part 659, State Oversight Agencies (SOAs) must require the rail transit agencies to develop and implement a written system safety program plan and system security plan that complies with requirements in 49 CFR part 659.

Part 659 requires SOAs to approve and annually review the rail transit agency system safety and security plans. Moreover, the SOAs must require covered agencies to develop and document a process for the performance of ongoing internal safety and security reviews as part of their plans. Finally, the SOAs themselves must conduct on-site reviews of system safety program plan and system security plan implementation.

The FTA has announced its intent to rescind part 659.[21] On March 16, 2016, the FTA published a safety-focused final rule, adding part 674 to their regulations to supersede part 659.[22] The safety requirements of part 674 took effect April 15, 2016. The FTA has stated its intent to rescind the security requirements in part 659 no later than April 15, 2019,[23] noting TSA's responsibility for rulemakings related to security of public transportation.[24] It also noted that RTAs may continue to implement measures to secure their operations and assets, but it is no longer the requirement of the SOAs to oversee those measures.[25]

The security measures that RTAs have implemented because of requirements under part 659 may be similar to what TSA proposes within the parameters set by the 9/11 Act. As with freight rail, TSA anticipates that PTPR owner/operators may be able to use plans developed and implemented under these DOT regulatory requirements to satisfy a portion of TSA's VASP regulations.

3. Emergency Preparedness Plans

The Federal Railroad Administration (FRA) safety standards require emergency preparedness plans by railroads connected with the operation of passenger trains

[21] See 81 FR 14230 (Mar. 16, 2016) (adding part 674 to title 49 of the CFR).
[22] Id.
[23] Id.
[24] Id. at 14233.
[25] Id.

(including freight carriers hosting passenger rail operations). Under 49 CFR part 239, these railroads must implement emergency preparedness plans that include: communication measures (including notification to on-board crewmembers and passengers about the nature of the emergency and control center personnel of outside emergency responders and adjacent rail modes of transportation); passenger evacuation in emergency situations; employee training and qualification; joint operations; tunnel safety; liaison with emergency responders; on-board emergency equipment; and, passenger safety information. In the Security Training NPRM, TSA proposes to allow training required by 49 CFR 239.101(a)(2) to be combined with other training in order to partially or fully meet requirements under § 1580.115(f) or § 1582.115(f) of that NPRM.[26] TSA expects that portions of the emergency response plans developed under part 239 could be equally relevant for satisfying some of the VASP requirements.

D. 17 Security and Emergency Action Items

Following the events of September 11, 2001, FTA developed security and emergency preparedness resources and provided technical assistance to transit agencies across the United States, including the "Top 20 Security and Emergency Preparedness Action Items for Transit Agencies" (published in 2003). In 2006, FTA and TSA collaborated to update and consolidate the FTA list into 17 Security and Emergency Preparedness Action Items for Transit Agencies (17 SAIs).

In 2012, FTA and TSA revised the 17 SAIs to ensure alignment with changes TSA was implementing in its assessment program. These changes added cyber-security as a topic, replaced the color-coded Homeland Security Advisory System (HSAS) with

[26] Titled "Security Training Programs for Surface Transportation Employees," published elsewhere in this issue of the Federal Register.

the National Terrorism Advisory System (NTAS), and revised and highlighted the priorities of risk management and risk information gathering and analysis. All changes reflected consultation with the industry through TSA's Mass Transit Sector Coordinating Council, chaired by the American Public Transportation Association (APTA).

The 17 SAIs reflect the high-level priority topics included in a security and emergency preparedness program, appropriately scaled to risk environment and operations. Table 1 identifies the current 17 SAIs.

Table 1. 17 Security and Emergency Preparedness Action Items

Management and Accountability …….	1. Establish written system security programs (SSPs) and emergency management operations/response plans. 2. Define roles and responsibilities for security and emergency preparedness. 3. Ensure that operations and maintenance supervisors, forepersons, and managers are held accountable for security issues under their control. 4. Coordinate security and emergency operations/response plan(s) with local and regional agencies.
Security and Emergency Response Training ……...	5. Establish and maintain a security and emergency training program.
National Terrorism Advisory System (NTAS) ……	6. Establish plans and protocols to respond to the NTAS alert levels.
Public Awareness …….....	7. Implement and reinforce a public security and emergency awareness program.
Risk Management and Information Sharing ……...	8. Establish and use a risk management process.
Risk Information Collection and Sharing ……	9. Establish and use an information sharing process for threat and intelligence information.
Drills and Exercises …….....	10. Conduct tabletop exercises and functional drills.
Cybersecurity ……...	11. Develop a comprehensive cyber-security strategy.
Facility Security, Access Controls, and Background Investigations ……..	12. Control access to security critical facilities with identification (ID) badges for all visitors, employees, and contractors. 13. Conduct physical security inspections. 14. Conduct background investigations of employees and contractors.
Document Control ……...	15. Control access to documents of security critical systems and facilities. 16. Process for handling and access to SSI.
Security Program Audits …….	17. Establish and conduct security program audits.

E. Baseline Assessment for Security Enhancement Program

In 2006, TSA established the BASE program, through which TSA inspectors conduct a thorough security assessment of public transportation agencies, passenger railroads, bus companies, and trucking companies. To conduct an assessment, inspectors ask a series of questions to develop a "snapshot" of current security measures (questions are slightly different for each mode). Within the relevant SAI categories, TSA applies numerical values to the level of implementation of an effective security measure. Final SAI scores quantify the entity's comprehensive transportation security posture.

TSA collaborates with owner/operators to develop options that could help mitigate a security-related vulnerability relative to the industry standard and identifies resources that TSA or other areas of the Federal government can provide to support raising the security baseline. The results of these assessments inform TSA policies and development of best practices to align such policy and program priorities with industry-wide security weaknesses. For example, during the interaction with owner/operators as part of a BASE assessment, TSA obtains information about whether specific measures for addressing identified issues are feasible within the specific-type of operation. TSA uses this information to develop alternative tools to enhance security. As TSA identifies industry-wide security weaknesses, the information informs priorities, policies, and programs. For example, TSA has used BASE statistics to recommend funding priorities to FEMA in an effort to ensure allocation priorities are consistent with identified industry-wide security weaknesses in light of current risks. In 2007, TSA's review of the industry-wide scores in the training category of the BASE assessments indicated

deficiencies. Based on this information, DHS prioritized frontline employee training within the Transit Security Grant Program (TSGP).

In FY 2011, TSA's review of BASE scores and discussions with industry revealed deficiencies at nationally critical infrastructure assets that were not being addressed at all, or as quickly as they could be. TSA worked with FEMA to overhaul the TSGP framework to prioritize these assets ("Top Transit Asset List") for funding through a wholly competitive process.[27] DHS subsequently awarded over $565 million to protect critical infrastructure assets. This funding resulted in increased preventive security for over 80 percent of nationally critical infrastructure assets.

In addition, as an initial requirement for grant eligibility, applicants must validate they have an updated security plan based on a security assessment, such as the BASE. They then must align all requests for funding (investment justifications) with items identified in the security assessment or security plan.

In FY 2015, TSA Inspectors completed 92 BASE assessments on mass transit and passenger rail agencies, of which 13 resulted in Gold Standard Awards for those entities achieving overall excellence in security program management. In 2012, TSA expanded the BASE program to the highway and motor carrier[28] mode and has since conducted over 400 reviews of highway and motor carrier operators, with 98 reviews conducted in FY 2015. On average, TSA conducts approximately 150 reviews on mass transit and highway and motor carrier operators each year, with numerous reviews in various stages of completion for FY 2016.

[27] See FEMA, "FY 2012 Transit Security Grant Program," available at https://www.fema.gov/fy-2012-transit-security-grant-program.
[28] See 77 FR 31632 (May 29, 2012) (60-day notice for Information Collection Request (ICR) for more information on expanding the BASE to highway and motor carrier transportation).

F. Transportation Security Template and Assessment Review Toolkit

The Transportation Security Template and Assessment Review Toolkit (T-START) is a resource created by TSA to assist owner/operators in developing effective security practices and in the construction of a security plan. The current version of T-START incorporates the BASE assessment for the highway mode. It is available for small companies, political subdivisions, or governmental entities having ownership or control over large systems (such as school buses), and large companies with national coverage. T-START currently includes five modules that walk the owner/operator's representative through the process of understanding security management and risk, a tool for conducting assessments, identification of risk-reduction, or mitigation options through awareness of industry "best practices" and other options developed by TSA, and a template for developing a security plan, the final crucial step toward an effective security program. T-START is currently scoped to address highway transportation security issues.

G. Security Measures and Resources Toolbox

The Security Measures and Resources Toolbox (SMARToolbox) is a resource to help surface transportation professionals identify relevant insights, security measures, and smart practices to increase their security baseline. The SMARToolbox is not a set of standards, rules, or regulations; rather, it is a compilation of smart security practices developed by industry, for industry across all modes of surface transportation. The heart of the SMARToolbox is a searchable, modifiable database of security measures identified by surface transportation professionals as valuable to their organization's operations. The SMARToolbox aligns security measures with category filters to allow for various

searches by, among other things, mode, threat scenario, and core capability. TSA intends this database to be a resource for the industry to assess the value of implementing various security measures into transportation systems. To augment the usefulness of the security measures database, the SMARToolbox also offers resources designed to facilitate implementation of the measures (for example, implementation checklists and self-assessment functions).

H. Terrorism Risk Analysis and Security Management Plan Developed by the Association of American Railroads

As an industry, the railroads have undertaken efforts to enhance the security and resiliency of the freight rail transportation system. In the aftermath of the 9/11 terrorist attacks, the railroad industry worked closely with local, State, and Federal officials and used their own police forces; the railroads increased inspections and patrols, restricted access to key facilities, briefly suspended freight traffic in the New York City area, and changed certain operational practices as anti-terrorist measures.

The Association of American Railroads (AAR) developed the Railroad Risk Analysis and Security Plan (AAR Plan) in April 2003 in response to the terrorist attacks, and as a proactive measure in collaboration with DHS to address perceived security vulnerabilities within the freight rail system. TSA anticipates that freight railroad owner/operators who have participated in this AAR initiative would use the results of those security assessments to expedite their compliance with the proposed requirements in the VASP regulations.

The AAR created five critical action teams, each for a specific area of concern within the rail industry.[29] The critical action teams examined and prioritized all railroad assets, vulnerabilities, and threats, and identified countermeasures. As part of the AAR Plan, the industry developed four threat-based alert levels, laying out progressively higher levels of action for the industry to implement in the event of certain security situations.

The AAR Plan provides an overall framework for industry-wide security measures while leaving the actual implementation up to each individual railroad carrier. Carriers used the plan as a guidance document to create security management plans for their respective company addressing their unique security concerns. The industry sees the AAR Plan as a living document reflecting changes in risk. As appropriate based on a continuous risk assessment process, they update and revise the plan.

I. Best Practices Developed by the American Public Transportation Association

APTA has instituted a Standards Development Program. Four working groups within the program have developed security oriented recommended practices for use by public transit agencies. The four working groups are focused on the following issues:

- Control and Communications Security;
- Emergency Management;
- Enterprise Cybersecurity; and
- Infrastructure & Systems Security.

[29]These action teams focus on critical security issues for railroad systems, including hazardous materials, information technology, communications, and military movements.

Through these working groups, APTA has published white papers and recommended practices.[30]

J. Security and Emergency Preparedness Plans

Both the commercial bus industry and public transportation agencies have created documents, which they named "Security and Emergency Preparedness Plans (SEPP)." Commercial OTRB companies created and distributed the OTRB SEPP in 2005. This document contained a proposed security assessment matrix and a template for creation of a company-wide security plan. TSA used the SEPP as the foundation for the T-START, discussed in section III.F.

In 2008, APTA released a SEPP with recommended security practices for public transit agencies and guidance for the creation of agency security assessments and protective plans. Both of these resources optimize–within the constraints of time, cost, and operational effectiveness–the protection of employees and passengers.

The SEPP meets several objectives: (1) achieving a level of security performance and emergency readiness that meets or exceeds the needs of similarly-sized operations; (2) increasing and strengthening a company's involvement in safety and security; (3) developing and implementing an assessment program focused on improving physical security and emergency response; (4) expanding security awareness and emergency management training for employees, volunteers, first responders, and contractors, and (5) enhancing security and emergency preparedness coordination with applicable local, State, and Federal agencies.

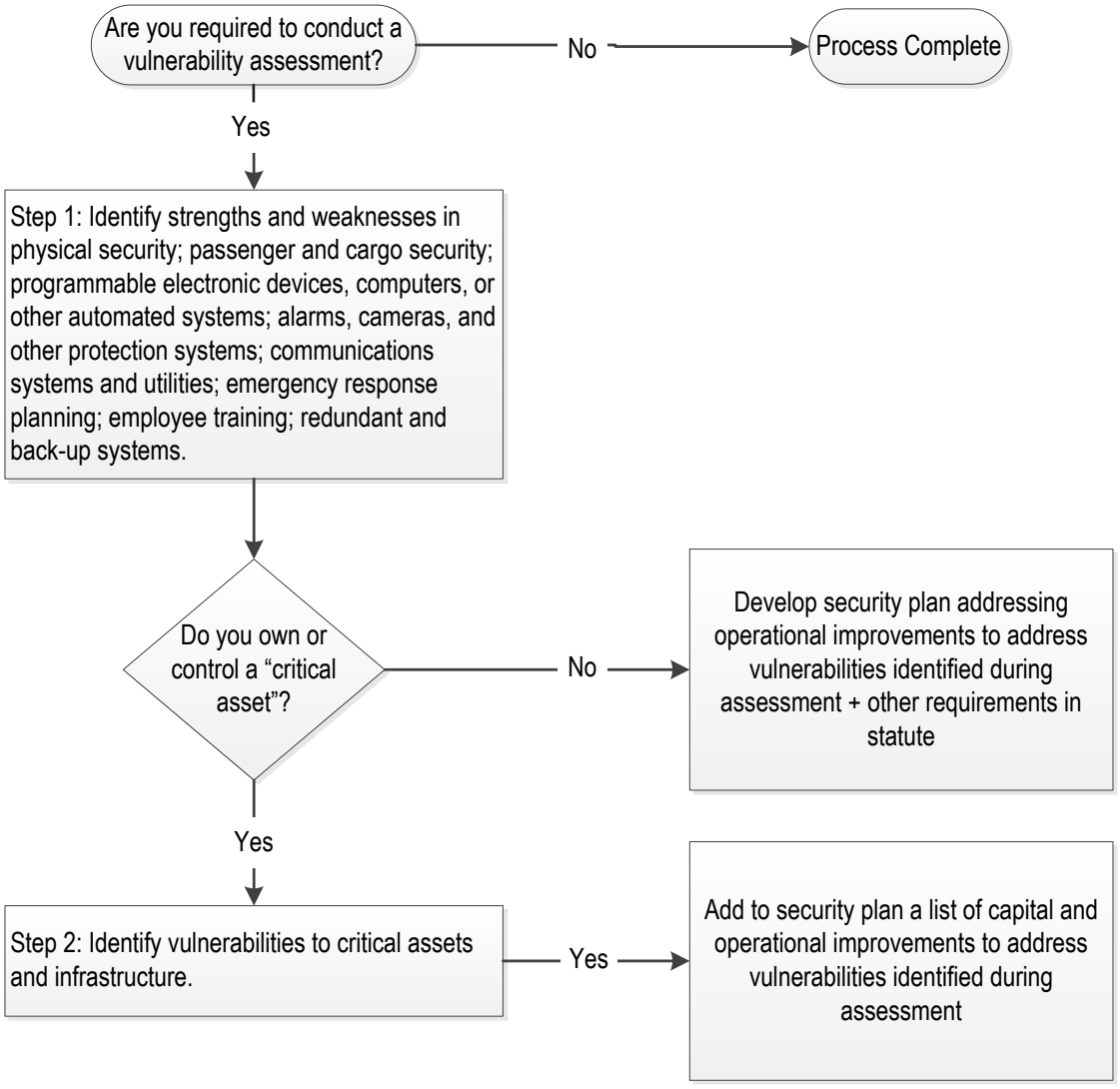
[30] More information on these standards can be found at http://www.apta.com/resources/standards/Pages/default.aspx.

IV. Assessments

A. General

The 9/11 Act's requirements for "vulnerability assessments" address both operations and assets. As shown in Diagram A, conducting such an assessment is a two-step process: (1) assessments of security systems and operations and (2) assessments of critical assets.

Diagram A: Assessment to Planning Process



TSA understands that submitting information about weaknesses in security systems/operations and critical asset protection may raise concerns regarding the public availability of the information. Under TSA's regulations for SSI,[31] all vulnerability assessments "directed, created, held, funded, or approved by" TSA are SSI.[32] Similar provisions apply to security programs or contingency plans "issued, established, required, received, or approved" by TSA.[33] Generally, access to SSI is strictly limited to those persons with a need to know, as defined in 49 CFR 1520.11, and to those persons to whom TSA grants specific access authorization under 49 CFR 1520.15. Pursuant to statute,[34] there is limited access to specific SSI in Federal district court proceedings to civil litigants who do not otherwise have a need to know under part 1520. This requirement only affects TSA's application of its non-disclosure policy in civil proceedings in Federal district court; it does not affect TSA administrative, State, or other Federal proceedings.

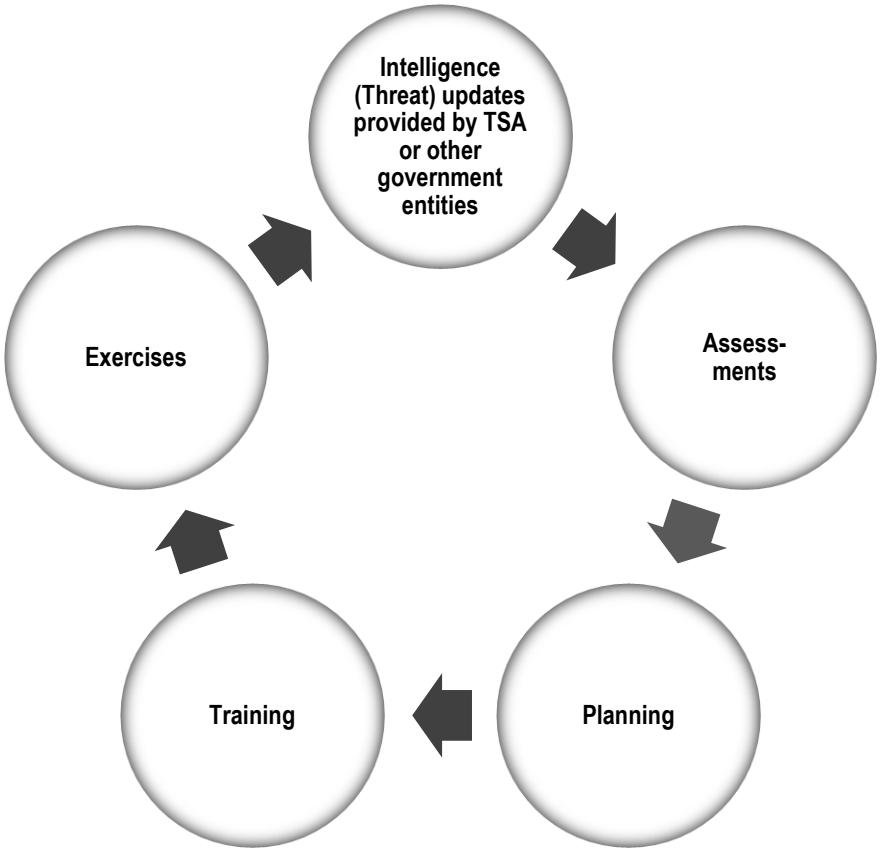
B. Assessments of Security Systems and Operations

A vulnerability assessment of security systems and operations is the foundation for an effective security program, including understanding the threat, identification of risk-reduction or mitigation measures, resource allocation decisions, employee training, drills and/or exercises to test preparedness and planning, and reassessments to determine

[31] See 49 CFR part 1520.
[32] Id. at 1520.5(b)(5).
[33] Id. at 1520.5(b)(1).
[34] See Department of Homeland Security Appropriations Act, 2007, Pub. L. 109-295, sec. 525(d), 120 Stat. 1355 (Oct. 4, 2006). Section 525 is uncodified, but Congress has reenacted the provisions in sec. 525(d) in each subsequent Department of Homeland Security Appropriations Act. Currently, the provision can be found at Pub. L. 114-113, div. F, sec. 510(a), 129 Stat. 2242, 2513 (Dec. 18, 2015, continued to December 9, 2016), by the Continuing Appropriations and Military Construction, Veterans Affairs, and Related Agencies Appropriations Act, 2017, and Zika Response and Preparedness Act, Pub. L. 114-223, sec. 101(6) (Sept. 30, 2016).

areas for change or improvement. As noted in Diagram B, assessment is part of a cyclical process.

Diagram B. Security Program Process



Collecting and analyzing information on deficiencies and weaknesses is a critical first step in managing and mitigating risks as it enables surface owner/operators to detect and manage security vulnerabilities. As assessment results, current intelligence/threat and other relevant information, and after-action reports of drills/exercises is fed into the planning cycle, surface owner/operators can better direct resources towards effective risk management.

C. Identifying Performance Standards for Assessments of Security Systems and Operations

TSA considers the BASE to be an important resource for developing the VASP regulations. The scope of the BASE program is fundamentally consistent with the 9/11 Act's requirements for assessments of security systems and operations.[35] Using the categories identified in Table 1 for the 17 SAIs, Table 2 crosswalks the categories for the 17 SAIs with the 9/11 Act's requirements for security assessments. In addition, the program and the assessment questions are familiar to many of the owner/operators who may be subject to these regulations.[36]

Table 2. Crosswalk Between 9/11 Act Assessment Requirements and 17 SAIs

9/11 Act Requirement	17 SAIs Category
Identification and evaluation of emergency response planning and other vulnerabilities related to passenger/cargo security ……... …….	Risk Management and Information Sharing
Identify weaknesses in emergency response planning related to passenger/cargo security …….	Management and Accountability National Terrorism Advisory System (NTAS) Public Awareness Risk Information Collection and Sharing
Identify weaknesses in employee training and emergency response planning …….	Security and Emergency Response Training Drills and Exercises
Identification of weaknesses in the security of programmable electronic devices, computers, or other automated systems; alarms, cameras, and other protection systems; and communication systems and utilities needed for security purposes …….	Cybersecurity
Identification of vulnerabilities to critical assets and infrastructure and weaknesses in physical security	Facility Security, Access Controls, and Background Investigations

[35] The current PTPR BASE is based on the 17 SAIs developed jointly by FTA and TSA. The highway BASE has 20 SAIs. In the past, TSA conducted Corporate Security Reviews (CSRs) for freight railroads, which were similar to the BASE. The CSR had fewer items. While the numbers may vary, the issues are generally the same (with the exception of some issues unique to a particular mode). Therefore, for purposes of this ANPRM, TSA will use 17 SAIs as a generic term for all of them.

[36] TSA is providing an appropriately detailed sample of questions in the docket for this rulemaking for commenters who are not familiar with the BASE.

While the questions used for a BASE assessment do not establish or identify performance standards, they could be the starting point for developing appropriate performance standards. For example, the 9/11 Act requires an assessment of strengths and weaknesses in emergency response planning. Currently, the BASE includes the following "yes" or "no" questions relevant to this requirement:

- Does the plan address personnel security, facility security, vehicle security, and Threat/Vulnerability Management?
- Does the plan include methods to identify and actively monitor the goals and objectives for the security program?
- Does the plan include a written policy statement that endorses and adopts the policies and procedures of the plan? Does top management, such as the agency's chief executive, approve and sign the plan?
- Does the plan address protection and response for critical systems?
- Does the plan clearly identify responsibilities (or reference other documents establishing procedures) for the management of security incidents by the operations control center (or dispatch center) or other formal process?
- Does the plan clearly identify (or reference other documents establishing) plans, procedures, or protocols for responding to security events with external agencies (such as law enforcement, local EMA, fire departments, etc.)?
- Has the owner/operator partnered with local law enforcement/first responders to develop active shooter procedures or protocols?
- Does the security plan contain or reference other documents that establish procedures or protocols for responding to active shooter events?

- Does the security plan contain or reference other documents that establish protocols addressing specific threats from: (1) Improvised Explosive Devices (IED), and (2) Weapons of Mass Destruction (chemical, biological, radiological hazards)?
- Does the security plan integrate visible, random security measures, based on employee-type, to introduce unpredictability into security activities for deterrent effect?
- Does the security plan require consideration of security before implementation of extensions, major projects, new vehicles and equipment procurement, and other capital projects?
- Does the security plan include or reference other documents adopting Crime Prevention Through Environmental Design (CPTED) or similar security-focused preventive principles as part of the agency's engineering practices?
- Does the security plan require an annual review?
- Does the owner/operator produce periodic reports reviewing its progress in meeting its security plan goals and objectives?
- Has the company conducted, and documented, an annual review of the security plan within the preceding 12 months?
- Does the security plan outline a process for securing review for updates and necessary approval of updates to the security plan?

Beginning with these "yes" or "no" questions, TSA could develop qualitative standards to help a surface owner/operator determine whether its security measure is weak, adequate, or strong based on how effective it is. Answers to those questions would

help the surface owner/operator identify weaknesses in its security measures and inform development and prioritization of risk-reduction measures.

For surface owner/operators that have conducted vulnerability assessments of security systems/operations, TSA seeks comment on the following questions:

1. Have you conducted a vulnerability assessment of your security system/operations within the last three (3) years?

2. If yes, did TSA conduct the assessment as part of the BASE program? If not TSA, did an independent auditor or company employees conduct the audit? How long did it to take to perform this assessment? How many individuals were involved in conducting the assessments (please provide information on the time and personnel costs for those essential to the assessment process, such as man-hours, permanent employees or contractor cost, etc.)?

3. How frequently do you update assessments of security systems/operations? Do you have internal or other requirements to update assessments? Are these requirements based on a schedule or changes to operations, assets and infrastructure, or threat information? How much time do these updates take?

4. Was the assessment of security systems/operations site-specific, system-wide, or both?

5. What resources or tools did you use for conducting your assessment?

6. What features of those resources or tools were most useful?

7. If the evaluation assesses operational security processes, such as training and operations, what methodologies or criteria are used to evaluate these processes?

8. What types of questions or other criteria were used to help identify strengths and weaknesses? Which of these were most relevant to your operations?

9. Do you use the results of the assessment for developing security plans, or emergency response plans, continuity of operations plans, etc.? Please describe how the assessment is used.

10. Was the assessment conducted in order to meet other Federal requirements (such as grant eligibility) or other standards? If so, please provide a description or source for those requirements or standards?

11. How can other required assessments addressing security systems/operations be used to satisfy TSA's regulatory requirements? For example, how relevant are FRA emergency preparedness requirements, PHMSA security plan requirements, and FTA's requirements? What standards should TSA use to determine if those plans meet TSA's requirements?

12. How could TSA ensure a surface owner/operator is in compliance with other agency requirements if it permits those measures to satisfy the requirements of TSA's regulation?

13. What barriers and/or challenges to conducting this assessment did you encounter?

D. Determination of Critical Assets and Infrastructure

As previously noted, the 9/11 Act requires a vulnerability assessment of critical assets/infrastructure. The statute does not provide criteria for determining whether an

asset is "critical."[37] Depending on the criteria, TSA could either require surface owner/operators to self-determine critical assets/infrastructure or inform surface owner/operators of a TSA-determination of criticality. The different approaches have significant impacts on the cost/benefits of vulnerability assessments, as well as the scope of required risk-reduction measures implemented as part of a security plan.

Self-determination of critical assets would require surface owner/operators to determine whether an asset is critical. Such a process would likely require owner/operators to first identify all of their assets (at least in the categories identified by the 9/11 Act) then use TSA-provided criteria to determine if any of those assets are critical. TSA would need to provide a tool or other measures to ensure consistent application of the criteria across all regulated parties.

A self-determination approach to criticality is likely to capture assets that may be critical from a business perspective, but not necessarily critical from the perspective of national security. This is a significant cost issue as identification of critical assets carries with it the regulatory burden to conduct a vulnerability assessment of the asset and implement appropriate risk-reduction measures to address any identified vulnerabilities, even if the asset is not critical from a national security perspective.

To address this concern, TSA could limit the requirement to "nationally critical assets and infrastructure" as determined by TSA. This determination would begin with a definition of national criticality. While there have been many efforts to define critical infrastructure and refine lists of critical assets in order to apply the appropriate protective measures since the terrorist attacks of 9/11. TSA finds the definition in Uniting and

[37] The 9/11 Act includes a list of critical asset types to be considered, as appropriate, but does not describe the criteria that would make them "critical." See 9/11 Act secs. 1405(a)(3)(A), 1512(d)(1)(A), and 1531(d)(1)(A).

Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001[38] has particular resonance as it was developed within the context of protecting assets from terrorist attack:

> In this section, the term "critical infrastructure" means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[39]

This definition was adopted by reference in the Homeland Security Act of 2002[40] and is used for the definition of "critical infrastructure" in the Presidential Policy Directive (PPD) on "Critical Infrastructure Security and Resilience" (PPD-21, issued Feb. 12, 2013) which replaces Homeland Security Presidential Directive 7.

Within the scope of such a definition, TSA would need to consider the criteria necessary for identifying nationally critical assets. For purposes of identifying a list of "nationally significant surface critical infrastructure," TSA has developed similar criteria in consultation with intelligence analysts and the industry. Such criteria consider location of the asset and the direct consequences of an act that incapacitates or destroys the asset.

Other possible criteria for consideration include those developed under the National Critical Infrastructure Prioritization Program (NCIPP). Identification and prioritization of critical infrastructure for purposes of the NCIPP consider the destruction or disruption of infrastructure that could have catastrophic national or regional consequences. This determination provides the foundation for infrastructure protection and risk reduction programs and activities executed by DHS and its public and private

[38] Pub. L. 107-56, 115 Stat. 272 (Oct. 26, 2001).
[39] Id. at sec. 1016(e) (codified at 42 U.S.C. 5195c(e)).
[40] Pub. L. 107-296, sec. 2(4), 116 Stat. 2135, 2140 (Nov. 25, 2002) (codified at 6 U.S.C. 101(4)).

sector partners. Table 3 provides the considerations for Level 1 and Level 2 under the NCIPP.

Table 3. NCIPP Categories

Impact	Level 1 (All Sectors)	Level 2 (All Sectors Excluding Agriculture and Food)
Casualties ……...	Greater than 5000 prompt fatalities	Greater than 2500 prompt fatalities
Economic Consequences ……...	Greater than $75 billion in first year	Greater than $25 billion in first year
Mass evacuations ……...	Prolonged absence of greater than 3 months	Prolonged absence of greater than 1 month
Security capabilities ...….....	Severe degradation of Nation's national security capabilities including intelligence and defense functions, but excluding military facilities	

For purposes of this rulemaking, surface owner/operators would only be notified if they owned or controlled an asset identified by TSA as nationally significant. For example, surface owner/operators may not own or have any operational control over the stations, terminals, or bridges they use for their operations.[41]

But TSA also recognizes that lack of ownership or control does not obviate the need to consider security. Operations of a surface owner/operator may rely on transportation infrastructure at risk based on its iconic significance. That risk could also apply to those who use it. While the surface owner/operator may not be able to reduce the risk for the asset, it can take measures to reduce the risk for its system when using that asset.

[41] Notwithstanding its authority to regulate all aspects of the transportation system, there are no current plans to apply the requirements to entities not identified as surface owner/operators in the Security Training NPRM.

TSA seeks comments on the following questions:

14. Should TSA use other standards to determine criticality? If so, please provide alternative standards.

15. If alternative standards were provided in response to Question 14, what types of assets or infrastructure would be determined as critical using the alternative standards? Answers containing SSI should be submitted according to the directions under SUPPLMENTARY INFORMATION.

16. Would the alternative standards provided in response to Question 14 result in a criticality designation for any or all of the assets and infrastructure identified in secs. 1512(d)(1)(A) and 1531(d)(1(A) of the 9/11 Act? See docket for this rulemaking for a table that aligns the 9/11 Act's requirements across the three modes.

17. If TSA were to adopt a broader list of assets and infrastructure–such as all of those identified in secs. 1512(d)(1)(A) or 1531(d)(1)(A) of the 9/11 Act–are some inappropriate for inclusion because the cost associated with assessments and planning would result in a corresponding benefit to surface transportation security? Are there some that are rarely, if ever, under the ownership or control of the owner/operators that would be subject to the rule's requirements?

18. What type of information and technical assistance would you need from TSA to facilitate conducting a vulnerability assessment?

For entities currently conducting self-determinations of critical assets and infrastructure, TSA seeks comments on the following questions:

19. How do you make the determination of criticality? For example, should TSA use criteria such as traffic volume (such as ton-miles over or through, passenger trains,

daily ridership, and/or number of shipments) or some other criteria associated with network criticality?

20. What is the cost of this process (how many hours, permanent employee or contractor, are required, etc.)?

21. Do you use the determination of criticality for development of general continuity of operations plans?

E. Identifying Performance Standards for Assessments of Critical Assets and Infrastructure

While there are many ways to complete an intelligence driven, risk-based vulnerability assessment for critical assets, they all rely on some form of subjective ranking system to identify and evaluate specified strengths and weaknesses. For example, a surface owner/operator could prioritize the threats relative to the asset as highly likely, somewhat likely, possible, unlikely, or improbable. Such owner/operator could then rate vulnerabilities (perhaps on a scale from very low to high), based on subjective decisions regarding how easy it would be to exploit that vulnerability given current operations. The owner/operator could also rate the consequence based on the type of threat. Combining all three ratings into an overall risk score helps identify the greatest risks in order to focus energies and limited resources on related vulnerabilities.

TSA is seeking information on appropriate resources that can inform development of performance standards for vulnerability assessments. Known resources include DHS tools, such as the framework of the Integrated Rapid Visual Screening (IRVS); issues addressed in questions related to asset protection that are part of a BASE assessment; and standards developed by the American Public Transportation Association (APTA).

For surface owner/operators that have conducted vulnerability assessments of critical assets and infrastructure, TSA seeks comments on the following questions:

22. Did you perform the vulnerability assessment on specific assets? If so, what assets? What criteria did you use to determine which assets to assess?

23. How long did it to take to perform this assessment? How many individuals were involved in conducting the assessments? Please provide information on the time and personnel costs for those essential to the assessment process, such as man-hours, permanent employees or contractor cost, etc.

24. Do you use the results of the vulnerability assessment for developing security plans, or emergency response plans, continuity of operations plans, etc.? Please describe how the assessment is used.

25. How frequently do you update vulnerability assessments? Do you have internal or other requirements to update assessments? Are these requirements based on a schedule or changes to operations, assets and infrastructure, or threat information?

26. Did you perform the vulnerability assessment in order to meet other Federal requirements (such as grant eligibility) or other standards? If so, please provide a description or source for those requirements or standards.

27. How can other required assessments be used to satisfy TSA's regulatory requirements? For example, how relevant are FRA emergency preparedness requirements or other DOT-modal requirements? What standards should TSA use to determine if that assessment meets TSA's requirements?

28. How could TSA ensure a surface owner/operator is complying with other regulatory requirements if it permits actions taken under those requirements to satisfy a

TSA regulation? For example, if a passenger railroad is required to develop and implement emergency evacuation planning under 49 CFR part 239 and wants to use that planning to satisfy a requirement that may be in the final VASP rule, how would TSA know whether the railroad is, in fact, complying with requirements imposed by the FRA? The fact that the FRA has not penalized an owner/operator for non-compliance is not a guarantee that the owner/operator is complying with the FRA requirements.

29. What barriers and/or challenges to conducting this assessment did you encounter?

V. Security Plans

Regulations imposing security plan requirements have a direct impact on operations. Thus, any rulemaking effort must recognize that measures beneficial to security may have a negative impact on operations. The purpose of this ANPRM is to solicit the input and data necessary for TSA to develop a proposed rule that ensures the level of security intended by the 9/11 Act without having an unintended impact on operations.

A. Identifying Performance Standards for Security Plans

For purposes of this ANPRM, TSA has grouped the 9/11 Act's specific requirements for security plans into the following categories:

- Results of security and vulnerability assessments and list of capital and operational improvements necessary to address identified vulnerabilities.
- Specific procedures to be implemented or used to prevent and detect unauthorized access to restricted areas designated by the owner/operator.

- Identification of measures to be implemented in response to emergencies or periods of heightened security, including—
    - A coordinated response plan that establishes 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;
    - 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
    - Additional measures to be adopted to address weaknesses in incident management identified during reviews, drills, or exercises testing emergency response.
- Identification of any redundant and backup systems that the owner/operator will use to ensure the continuity of operations of critical assets and infrastructure in the event of a terrorist attack or other transportation security-related incident.

As previously noted in Table 2, there is a correlation between the 17 SAIs and the 9/11 Act's requirements. As with the security assessment (covering security systems and operations), the quantitative questions used in the BASE could be used as a starting point for developing qualitative performance standards for security plans.

For surface owner/operators that have security plans, TSA seeks comments on the following questions:

30. Does your security plan address the issues discussed at the beginning of this section?

31. Is your security plan site-specific, system or corporate-wide, or both?

32. Did you use a vulnerability or similar assessment (BASE or other) to develop a security plan? If not BASE, please describe the assessment. If so, what is the process for incorporating the results into your planning process and development of risk-reduction or mitigation measures (or investment justifications for grant purposes)? What levels of management are involved in reviewing the results of the assessment and making decisions regarding security planning related to those results?

33. How long did it to take to develop the security plan? How many individuals were involved in the planning process? Please provide information on the time and personnel costs for those essential to the planning process, including man-hours, permanent employee and/or contractor cost, etc.

34. How frequently do you update your security plan? Do you have internal requirements to update plans based on a schedule or changes to operations, assets and infrastructure, or threat information?

35. Does your security plan exist in order to meet other Federal requirements (such as grant eligibility) or other standards? If so, please provide a description or source for those requirements or standards.

36. How can other required plans be used to satisfy TSA regulatory requirements? For example, how relevant are FRA emergency preparedness

requirements, PHMSA security plan requirements, and FTA's requirements? What standards should TSA use to determine if those plans meet TSA's requirements?

37. How could TSA ensure a surface owner/operator is in compliance with other agency requirements if it permits those measures to satisfy the requirements of TSA's regulation?

38. What barriers or challenges to developing and implementing a security plan did you encounter?

B. Tools and Other Resources

TSA is considering modifying T-START to provide a resource to owner/operators subject to the VASP regulations. As discussed in section III.F of this ANPRM, T-START currently includes several modules that cover the assessment and planning cycle for the highway mode. The revised T-START would include modules consistent with requirements TSA incorporates into a final VASP rule and be applicable to PTPR and freight railroads, with modules that are relevant to the specific type of operation. TSA would provide this tool at no cost to surface owner/operators. For those not within the scope of applicability, T-START would provide guidance to them for conducting assessments and developing plans.[42]

TSA seeks comments on the following questions:

39. Have you used T-START to conduct assessments or develop a security plan?

40. What features of T-START or other resources or tools were most useful?

[42] The 9/11 Act requires TSA to provide guidance to owner/operators not within the high-risk tier. See 9/11 Act secs. 1512(b)(1) and 1531(b)(1).

41. Did the availability of T-START or other similar resources reduce the time necessary to conduct assessments or develop security plans? If so, please provide an estimate of the savings in time and personnel.

42. What other types of information, tools, and/or technical assistance could TSA provide to facilitate compliance with the VASP regulation? If you identified barriers or challenges in conducting vulnerability assessments or developing/implementing security plans in response to questions 13, 29, and/or 38, please provide specific suggestions on how TSA could provide information, tools, or other technical assistance in overcoming those barriers and/or challenges.

43. If you have not used T-START, please describe the programs, tools, or resources you have used.

44. Are there assessment/planning tools or resources that TSA should consider as relevant for developing the VASP proposed rule? If so, please provide names and sources.

C. Risk-Reduction or Mitigation Measures

As previously noted, the 9/11 Act specifies that security plans must include results of security and vulnerability assessments and list of capital and operational improvements necessary to address identified vulnerabilities.

TSA seeks comments on the following questions:

45. What security measures have owner/operators implemented to address weaknesses in either security of systems/operations or security of critical assets relevant to the requirements of the 9/11 Act (for example, measures to strengthen security of systems/operations and equipment).

Table 4. List of Possible Risk-Reduction or Mitigation Measures.

Cameras (please provide information on the brand, model, requirement, etc.) ……..	Speakers (public address systems or emergency communication systems)
Employee background checks ……..	Access control (such as Jersey barriers, automated gates, etc.)
Lighting ……	Dedicated law enforcement or other security personnel
ID card reader/badging systems ……...	Signage
Screening technologies (such as metal detectors, random baggage checks, etc.) ……..	Intrusion detection systems
Canine teams ……	Other (specify measure)

46. What data can you provide on the cost of purchase, implementation, and on-going maintenance of these measures, as appropriate? If possible, for each of the types of possible risk-reduction or mitigation measures identified in Table 4, please provide information on--

(a) Whether the company has installed this type of measure;

(b) How does the company use this measure (is it used randomly, in specific locations based on risk, or system-wide); and

(c) What are the costs associated with implementing this measure (purchase cost, installation, on-going maintenance, replacement, monitoring, etc.)?

47. Do your security measures include provisions for adding contracted security services in the event of elevated alert levels?

48. For those that have implemented security measures, can you provide data regarding implementation schedules (time between identification of the need, commitment to addressing it as part of planning, and actual full implementation or installation)?

49. What data sources are available for identifying industry standards relevant to implementation of risk-reduction or mitigation measures?

VI. Drills and Exercises

The 9/11 Act includes "[l]ive situational training exercises . . ." as a program element of the Security Training NPRM.[43] TSA decided not to include this requirement in the Security Training NPRM because it is inconsistent with the DHS methodology for exercises. The Homeland Security Exercise and Evaluation Program (HSEEP)–an exercise support program that focuses on the need to test planning and preparedness–focuses on the need to test effectiveness of the overall plan. By testing planning and preparedness, the drills and/or exercises reveal any weaknesses in training. Furthermore, the HSEEP does not require every exercise to be full-scale, live, and situational in order to be an effective test of the security plan. Many resources and methods are available to test the effectiveness of the plan and the preparedness of the organization and its employees to implement it other than full-scale, live, situational exercises. These range from seminars and workshops to basic or advanced tabletop exercises.

TSA is also concerned that a requirement to conduct live, situational exercises would impose a regulatory burden that owner/operators could not meet because they do not control all of the resources necessary for a live situational exercise, such as first responders, medical support, and other local and State government participation.

TSA seeks comments on the following questions:

50. To what extent do you have access to EXIS or other resources for conducting drills and/or exercises?

51. Have you participated in an I-STEP exercise?

[43] See secs. 1408(c)(7) (public transportation), 1517(c)(8) (freight rail), and 1534(c)(8) (OTRB).

52. Have you used EXIS as a resource for conducting drills and/or exercises?

53. If not through I-STEP or EXIS, how often do you conduct or participate in drills and/or exercises, what job positions participate, and what are the costs (development, implementation, after-action analysis, and reports)?

54. Based upon your experience with drills and exercises, are they an adequate method for assessing effectiveness of employee training, or are additional assessment tools needed for assessments?

55. Based on your experience, what are the most effective types of drills and/or exercises for testing preparedness, including identifying weaknesses in training?

56. Do you regularly use "after action reports" to modify security measures and procedures or make other operational or capital changes to improve security?

VII. Updates

The 9/11 Act specifies that owner/operators must update assessments and security plans on a regular basis. For public transportation, the 9/11 Act stipulates annual updates, including updates to assessments, improvement priorities, and security plans as appropriate. Eligibility for funding under the TSGP requires: (1) an assessment within three years before the request for funding, and (2) all requests for funding must be consistent with addressing vulnerabilities identified in that assessment. For railroads and OTRB owner/operators, the 9/11 Act requires updates to the assessment no later than three years after initial approval of the assessments or plans required in the regulation and at least once every five years after that date.

In a provision applicable to all aspects of the regulatory security program, the Security Training NPRM proposes requiring surface owner/operators to request

amendments to their programs (training, assessment, or planning) whenever there are changes to their operations, measures, training, or staffing. TSA would also be able to require updates if, for example, new threat information indicates the necessity of review and modification of security measures. TSA also anticipates the necessity for updates if there are significant changes to operations or assets, such as expanding operations, changes to routes, or modifications to hazardous materials designated as high-risk for transport.

TSA requests comments on the following questions:

57. How often do surface owner/operators update their assessments (either security systems/operations or critical assets)? Please include in your response information on the time and personnel costs for those essential to the updating process, such as man-hours, permanent employees or contractor cost, etc.

58. How frequently do these updates of assessments require changes to emergency response, safety, or security plans? If there are changes required, what types of changes do you typically make?

59. Are these updates required by other Federal or State regulations? If so, please provide a citation and any other relevant information regarding the requirement.

VIII. Accountable Executive

Every transportation system, whether plane, train, or bus, must make decisions for budgeting, allocating funds, and planning for the future. Recognizing the diversity of business organization and ownership represented by the scope of this rulemaking, TSA anticipates that the need to identify a decision-maker who has responsibility over the process for approving assessments and plans within the context of making decisions

regarding organization, operations, and allocation of resources. This "accountable executive," and any relevant boards or equivalent entities with which this individual may work, needs to have awareness of the risks (threats, vulnerabilities, and potential consequences) relevant to its security systems/operations and critical assets. Having responsibility to approve assessments submitted to TSA ensures this information can be used as part of informed, deliberate, and transparent decisions regarding the commitments made in the security plan.

Based on a review of how the term "accountable executive" is defined within various business contexts, TSA anticipates defining the term as a person responsible for implementation and security-related decisions, including allocation of corporate resources related to security. The "accountable executive" should be a single, identifiable person who has ultimate responsibility for the owner/operator's compliance with the security plan requirements, including obtaining written validation that the plan has been reviewed and approved by senior management (board of directors or equivalent entity). TSA also expects that this person will serve as the primary point of contact for TSA during the review and approval process of the security plan.

TSA seeks comment on the following questions:

60. Should the "accountable executive" be a chief executive officer or equivalent rather than an executive designated for this purpose?

61. For entities within the applicability proposed in the Security Training NPRM, do you have an accountable executive? What level is this person within the corporate structure? What other responsibilities does this person have? Do you have some other

process for ensuring senior management is made aware of the results of the assessment, approves its transmittal to TSA, and approves the security plan?

IX. Considerations for Small Owner/Operators

While TSA recognizes the administrative burden on small owner/operators,[44] the statute requires TSA to apply the requirements based on risk, not size of the operations. As a result, small PTPR systems that feed into larger systems covered by the applicability could be required to conduct assessments, develop a security plan, and implement related security measures. Similarly, the requirements could affect small OTRB owner/operators.

TSA anticipates that owner/operators of larger systems or fleets would develop an organization-wide approach for their assessments and plans, addressing different perspectives of operations, safety, planning, engineering, budget, and information technology along with the need to enhance and sustain security. TSA is considering whether owner/operators of smaller systems or operations would need to take a simpler approach in developing an assessment and plan and implementing security measures. If so, the regulation would need to consider owner/operators of smaller systems or operations could use information that is already largely on-hand or readily available to meet the same performance standards applied to larger companies.

TSA seeks comments on the following questions:

62. As TSA has determined that the higher-risk is associated with where the transportation occurs, not size of the company providing the transportation, what options

[44] The Small Business Administration (SBA) sets a threshold of $15.0 million in annual receipts for bus systems and mixed-mode transit systems, and 1,500 employees for short line railroads. See 13 CFR 121.201.

are there for minimizing the burden on small owner/operators without reducing the intended security benefit?

63. How should the VASP requirements apply to owner/operators who rely on the security of an asset or infrastructure owned by a third party?

64. What are the barriers for surface owner/operators with a smaller scope of operation–other than costs–to develop and implement a more comprehensive security program or plan with specific security measures, training, and assets?

65. How can TSA ensure consistent application of the standards or performance criteria of its rulemaking in light of the dynamic population to which the requirements would apply–large, small, publicly owned, small budgets, large tax-based budgets, etc.?

X. Estimating the Benefits and Cost of Requirements

Executive Orders 12866 and 13563 direct agencies to propose or adopt a regulation only upon a reasoned determination that its benefits justify its costs, tailor a regulation to impose the least burden on society consistent with obtaining the regulatory objectives, and in choosing among alternative regulatory approaches, select those approaches that maximize net benefits.

Consistent with the requirements in these executive orders, TSA seeks comment on the following questions:

66. For those who are already conducting vulnerability assessments and developing/implementing security plans, what are the security benefits? What would be the security benefits of a consistent, national standard for VASP?

67. TSA seeks information from the public in order to assist it in assessing the cost of alternative regulatory approaches for implementing the VASP regulations. For

example, for commenters who suggest that TSA consider adopting certain security performance criteria or objective standards for measuring the security of assets and infrastructure or security systems/operations, what information do you have to assist TSA in assessing the incremental cost of adopting your suggestion? TSA is interested in information to assist it in assessing the full cost of the suggestion, such as the cost for owner/operators to collect and assess information and the cost to take action based on the information.

68. Likewise, TSA seeks information from the public to assist TSA in assessing the potential benefits of alternative regulatory approaches for implementing the VASP regulations. For example, for commenters who suggest that TSA consider adopting certain security performance criteria or objective standards for measuring the security of assets and infrastructure or security systems/operations, what information do you have to assist TSA in assessing the incremental benefit[45] from adopting your suggestion?

69. What resources (for example, people, websites, organizations, companies) could be useful if TSA has difficulty obtaining accurate and timely data on public transportation systems, railroads, or OTRB modes necessary for developing a valid estimate of potential costs for compliance with a proposed VASP regulation? TSA specifically seeks data on employee wages, cost of equipment, and population data on companies within an industry or transportation mode.

XI. Next Steps and Public Participation

This ANPRM seeks input from the public on these topics to ensure that the NPRM to follow addresses all relevant information, provides the explanations necessary

[45] When requesting the assessment of an incremental benefit, TSA is referring to the additional benefits of the alternative the commenter is proposing compared to what TSA is proposing and compared to not taking any action at all.

to understand the proposed requirements, and appropriately estimates costs. It is important that freight railroad, PTPR, and OTRB owner/operators, other organizations, as well as interested members of the public potentially affected by a final rule, take this opportunity to share thoughts, concerns, ideas, and general comments on the topics presented.

After TSA reviews the comments collected through this ANPRM, TSA will prepare and publish an NPRM that reflects TSA's analysis of the statutory requirements and relevant issues, as well as comments received from the public through this ANPRM. Once TSA publishes the NPRM, stakeholders and the public will have another opportunity to provide comments that TSA will take into consideration before issuing a final rule.

Dated: November 18, 2016.

Huban A. Gowadia,

Deputy Administrator.

[FR Doc. 2016-28300 Filed: 12/15/2016 8:45 am; Publication Date: 12/16/2016]