2018 Biennial National Strategy for Transportation Security

Report to Congress

April 4, 2018

Homeland Security

Transportation Security Administration

Message from the Administrator

April 4, 2018

I am pleased to present the 2018 National Strategy for Transportation Security. This report is a forward-looking, risk-based plan to protect the Nation's transportation systems from terrorist attack over the period spanning 2018-2021. The Strategy was prepared pursuant to 49 U.S. Code 114(s), which requires a biennial update.

The Transportation Security Administration (TSA) led the development of the Strategy and the included modal and intermodal security plans with the joint participation of the Department of Transportation and in consultation with government partners and industry owners and operators.

While the Strategy presents a whole community plan for reducing the risks to transportation from terrorist attacks, it is, as mandated, the governing document for federal transportation security efforts.

The TSA, as the lead federal agency for transportation security, will exercise that leadership, both domestically and internationally, through: *(1) strengthening the effectiveness of TSA's aviation screening and in-flight security operations, (2) driving improvements in aviation security through enhanced standards and robust compliance regimes, (3) promoting partners' capabilities for protecting surface transportation systems, (4) expanding and improving intelligence and information sharing across mission areas, and (5) enhancing transportation vetting and credentialing operations.*

TSA intends to accomplish that by: *(1) focusing on core mission areas and aligning process and technology to front line officers, (2) establishing a common view of the threat we are operating to defeat, (3) strengthening strategic partnerships, connections to the intelligence community, and research, analysis, and operational capabilities to mitigate potential threats, (4) robust sharing of actionable information with partners, and (5) enhancing the fusion of known or suspected threat encounter information to provide real-time security threat awareness and drive vetting and screening activities.*

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Thune
Chairman, Committee on Commerce, Science, and Transportation

The Honorable Bill Nelson
Ranking Member, Committee on Commerce, Science, and Transportation

The Honorable Ron H. Johnson
Chairman, Committee on Homeland Security and Governmental Affairs

The Honorable Claire McCaskill
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable Mike Crapo
Chairman, Committee on Banking, Housing, and Urban Affairs

The Honorable Sherrod Brown
Ranking Member, Committee on Banking, Housing, and Urban Affairs

The Honorable Michael T. McCaul
Chairman, Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, Committee on Homeland Security

The Honorable William Shuster
Chairman, Committee on Transportation and Infrastructure

The Honorable Peter A. DeFazio
Ranking Member, Committee on Transportation and Infrastructure

The Honorable Mike Pence
President of the Senate

The Honorable Paul Ryan
Speaker of the House

The Honorable Mitch McConnell
Senate Majority Leader

The Honorable Chuck Schumer
Senate Minority Leader

The Honorable Nancy P.D. Pelosi
House Minority Leader

Inquiries relating to this report may be directed to me at (571) 227-2801 or TSA's Office of Legislative Affairs at (571) 227-2717.

Sincerely yours,

David P. Pekoske
Administrator

Executive Summary

The 2018 National Strategy for Transportation Security (the Strategy) addresses the security of "transportation assets in the United States that…must be protected from attack or disruption by terrorist or other hostile forces…."[1] The Strategy presents a forward-looking, risk-based plan to provide for the security and freedom of movement of people and goods while preserving civil rights, civil liberties, and privacy. It identifies objectives to enhance the security of transportation infrastructure, conveyances, workers, travelers, cargo, and operations. The Strategy includes a base plan, modal security plans, and an intermodal security plan. The base plan describes the risk-based foundation of the Strategy. The appended security plans provide mode-specific and intermodal activities to reduce terrorism risks and to protect transportation systems. The National Strategy for Public Transportation Security and the National Strategy for Railroad Transportation Security, required by the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), are included as annexes.[2] They provide a strategic context for the related modal plans in the appendices.

Guiding Principles: Four guiding principles provide an overarching framework for developing and implementing the Strategy.

1. **Agile, Adaptable Security Posture:** Intelligence and risk assessments and forward-looking threat analyses provide the foundation to define the priorities, objectives, and activities necessary to achieve strategic goals.

2. **Partnerships:** The responsibilities for transportation services—that provide the mobility necessary for insuring prosperity and our way of life—are broadly distributed among the whole community. The Strategy recognizes that building effective partnerships, in conformance with laws for receiving advice from non-government entities, is a government responsibility.

3. **Privacy and Civil Rights:** While striving to enhance transportation security, government and industry must preserve and protect the fundamental civil rights and civil liberties of the public they serve.

4. **Accountability:** Government and private sector security partners are accountable to the American people for the implementation of this Strategy and for reporting progress.

Strategic Environment: The Strategy takes into consideration the dynamic and adaptive nature of the terrorist threat. Transportation assets may be targeted by terrorists, used as weapons, or used to execute attacks. Current terrorism risks to transportation systems are historically associated with transnational and regional terror organizations such as al-Qa'ida and the Islamic State in Iraq and Syria. The Strategy assumes that the targets and attack methods used overseas provide insights regarding the aspirations of adversaries domestically. Emerging terrorism risks arise from the development of techniques or technologies that provide adversaries with new capabilities to conduct hostile operations.

---

[1] 49 U.S.C. § 114(s)(3)(A).
[2] 6 U.S.C. § 1133 and § 1161, respectively.

Challenges: Achieving security objectives in a resource constrained environment requires that security managers make risk-based choices to secure assets and systems. The uncertainties about the adversaries' intentions and capabilities complicates the program decisions and resource allocations that must be made. Should an attack occur in any sector, transportation services will be vital for response and recovery. Consequently, system resilience is an important aspect of the security equation. Evaluation of the many security issues across the diverse and dynamic spectrum of risks to transportation services presents significant challenges for measuring the effectiveness of risk mitigation activities.

Mission, Vision, and Strategic Goals: The mission statement unifies transportation security partners in a shared purpose. The vision statement is the end-state to be achieved by accomplishing the mission.

Mission: Secure the Nation's transportation system from acts of terrorism.

Vision: A secure and resilient transportation system, enabling travelers and goods to move freely without significant disruption of commerce or loss of civil liberties.

The Strategy identifies three strategic goals with supporting objectives that guide the priorities and activities in the modal security plans.

Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience.

Goal 2: Enhance effective domain awareness of transportation systems and threats.

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce.

Risk-Based Priorities: The Strategy applies a strategic risk-management approach to implement the goals. Risk management principles, including risk assessments and segmentation methods, form the foundation for identifying security priorities and the courses of action that provide cost-effective solutions to the risk of terrorist attacks.[3] Prevention of, and protection from, historic and emerging threats requires intelligence-driven assessments that detect attack patterns, current terrorist practices, and potential threats. Intelligence capabilities rely on vital information sharing among transportation operators, system users, security managers, and the

[3] The 2014 Quadrennial Homeland Security review identified a risk segmentation approach to securing and managing the flows of people and goods as a strategic priority. Populations or types of goods are considered as a group or segment based on provided information to facilitate selection of an appropriate security review procedure.

intelligence community. An alert and informed public provides an important force multiplier for intelligence and law enforcement efforts to prevent attacks by terrorists.

The threat of hijacking is still a concern. Attackers may employ a variety of tactics for the use of lethal weapons in transportation venues. Improvised explosive devices (IEDs) deployed in vehicles or hidden in backpacks or other innocuous packages or bags have been a common tactic. Transportation operations are also at risk of individuals or small teams of active shooters using IEDs, conveyances, knives, or a combination of weapons in single or coordinated attacks. Chemical, biological, radiological, or nuclear weapon threats are security priorities due to the potential consequences of such an attack.

Cybersecurity is a priority for the transportation community. Cyber systems used in transportation provide networked communications services; positioning; navigation; tracking capabilities and industrial control systems. These systems often have many data access points that expose the systems to intrusion. Terrorists or other criminals may exploit these vulnerabilities to disrupt operations, finance their nefarious activities, or glean valuable system or personal data.

Performance: The Transportation Security Administration (TSA) employs a variety of assessment tools to evaluate the security risks and posture of transportation providers. In addition, the Strategy identifies activity performance measures to indicate progress achieving intended outcomes. This progress is reported annually to Congress.

Path Forward: The Strategy identifies six opportunity areas to be considered in future security planning and programming: 1) enhanced use of risk-based assessments; 2) more effective use of information sharing products and platforms; 3) more effective use of security exercises; 4) better understanding of the transportation resilience in supply chains; 5) better understanding of cyber system vulnerabilities and consequences; and 6) better use of research and development initiatives to improve security effectiveness and efficiency and drive technological investment. Each area requires thoughtful collaboration to achieve a common understanding of challenges, impacts, and feasible solutions.

Transportation Operational Recovery Planning: Following an incident, transportation system recovery is essential to restore services to impacted communities and sectors. The Federal Government provides guidance for business continuity, local and regional preparedness, and response and recovery for transportation service providers.

Appendix A: 2018 Aviation Security Plan

The 2018 Aviation Security Plan identifies and addresses high-priority security risks to the assets and systems of the Aviation Transportation System that must be protected from disruption by terrorists or other hostile forces. Multiple aviation stakeholders and government agencies protect critical aviation assets and systems including the cyber, human, and physical elements of air cargo systems, commercial airlines and airports, general aviation, flight schools, and repair stations that are at the greatest risk of attack.

The aviation security risks are dominated by international and transnational terrorism. Terrorist threats against aviation include stand-off weapons, explosives, and chemical and biological weapons introduced on persons or in baggage. Techniques and tactics frequently evolve in response to security measures in place. Consequently, the aviation community relies on intelligence and risk analyses to determine security priorities to: 1) protect aviation physical assets and cyber systems; 2) optimize air domain awareness of domestic and international threats; and 3) improve aviation security worldwide through international partnerships and security cooperation.

Risk-based security practices, including risk segmentation techniques, apply the proper level of screening to travelers, baggage, and cargo. These techniques maintain security while enhancing the traveler's experience and expediting cargo handling. The proliferation of new technologies such as unmanned aircraft systems, the development of weapons and tactics that are more difficult to counter, and the persistence and adaptability of terrorists present continuing challenges to enhance procedures and capabilities to deter, detect, and prevent attacks.

Appendix B: 2018 Maritime Security Plan

The 2018 Maritime Security Plan presents risk-based priorities and activities to protect the Marine Transportation System (MTS) from terrorism and to enhance system recovery following a terrorist incident. The goals are to save lives, preserve property, and minimize disruption to the MTS.

The maritime mode includes ports, waterways, marine terminals, vessels serving a wide variety of commercial and recreational vessels, and numerous related government and industry operations to sustain maritime operations. Terrorism threats to the assets and systems of the MTS include IEDs, weapons of mass destruction, standoff weapons (such as man-portable air defense weapons and rifle-propelled grenades), and cyber-attacks. MTS assets may be targets of attackers or used to transport weapons in containers or cargo to other targets. Cruise ships and ferries are particularly susceptible to IED threats due to the high concentrations of people and the ease of concealing threats in baggage, cargo, or vehicles. Passenger vessels are also susceptible to attacks using small arms and biological or chemical agents. The U.S. Coast Guard's Maritime Security Risk Analysis Model assists maritime security managers in assessing strategic operational risks and establishing security priorities. These priorities include increased enforcement of Maritime Security Regimes, enhanced Maritime Domain Awareness, and risk-based deployment of Maritime Security and Response Operations.

Appendix C: 2018 Surface Security Plan

The 2018 Surface Security Plan includes four modal security plans for mass transit and passenger rail, freight rail, highway and motor carriers, and pipelines. Attacks using small arms or edged weapon, vehicle ramming, and IEDs are likely threats to the surface modes. Public transportation is particularly susceptible to attacks using standoff weapons and nuclear, radiological, biological, or chemical weapons. The surface

modes rely on cyber systems for tracking, signals, and operational controls. As dependence on cyber systems increases, so do the operational risks from cyber-attacks.

The surface modes share common security priorities to address common risks. TSA leads collaborative efforts to implement security assessments, planning, training, and exercises in high-risk transportation operations. Federal partners continue to provide and improve the timely sharing of useful intelligence and security information, to encourage the voluntary adoption of recommended best practices for cybersecurity, and to enhance detection and response capabilities.

Appendix D: 2018 Intermodal Transportation Security Plan

Global supply chains consist of a dense network of routes and carriers operating efficiently to provide time-sensitive deliveries. The 2018 Intermodal Transportation Security Plan focuses on protecting the movement of supplies and products within and across multiple modes of transportation. The Plan safeguards transportation links in the global supply chain from disruptions in the interest of commerce and national security.

Annexes

Annex I, the 2018 National Strategy for Public Transportation Security, addresses the requirements of the 9/11 Act, title 6 United States Code section 1133 (6 U.S.C. § 1133) to minimize the security threats to public transportation systems and maximize their abilities to mitigate damage resulting from an attack or other major incident.

Annex II, the 2018 National Strategy for Railroad Transportation Security, addresses the requirements of the 9/11 Act (6 U.S.C. § 1161) to improve the security of railroad infrastructure, facilities, information systems, and other areas that pose a risk to public safety or to interstate commerce including coordination with communities and commuter passenger rail operators to restore services quickly following attacks or other disruptions.

2018 Biennial National Strategy for Transportation Security

Table of Contents

I. Legislative Requirement

The 2018 National Strategy for Transportation Security addresses requirements in legislative, executive office, and departmental directives including, but not limited to, the following:

- *Intelligence Reform and Terrorism Prevention Act* (IRTPA) of 2004, Pub. L. No. 108-458 (December 17, 2004);
- *Aviation and Transportation Security Act*, Pub. L. No. 107-71 (November 19, 2001);
- *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), Pub. L. No. 110-53 (August 3, 2007);
- Presidential Policy Directive 8, National Preparedness (2011);
- Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (2013);
- Executive Order 13636, Improving Critical Infrastructure (2013);
- Homeland Security Presidential Directive-5, Management of Domestic Incidents (2003);
- National Strategy for Maritime Security and its supporting plans (2005);
- National Strategy for Aviation Security and its supporting plans (2007);
- National Strategy for Counterterrorism (2011);
- National Strategy for Global Supply Chain Security (2012);
- NIPP 2013, *Partnering for Critical Infrastructure Security and Resilience*; and
- 2014 Quadrennial Homeland Security Review (2014).

The IRTPA required the Secretary of Homeland Security to "develop, prepare, implement, and update" a National Strategy for Transportation Security.[4]

> (1) The Secretary of Homeland Security shall develop, prepare, implement, and update, as needed,
>
> (A) A National Strategy for Transportation Security; and,
>
> (B) transportation modal security plans addressing security risks, including threats, vulnerabilities, and consequences, for aviation, railroad, ferry, highway, maritime, pipeline, public transportation, over-the-road bus, and other transportation infrastructure assets.
>
> (2) Role of Secretary of Transportation. The Secretary of Homeland Security shall work jointly with the Secretary of Transportation in developing, revising, and updating the documents required by paragraph (1).
>
> (3) Contents of national strategy for transportation security. The National Strategy for Transportation Security shall include the following:
>
> (A) An identification and evaluation of the transportation assets in the United States that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces, including modal security plans for aviation, bridge and tunnel, commuter rail and ferry, highway, maritime, pipeline, rail, mass transit, over-the-road bus, and other public transportation infrastructure assets that could be at risk of such an attack or disruption.

[4] IRTPA § 4001, codified at 49 U.S.C. § 114(s).

(B) The development of risk-based priorities, based on risk assessments conducted or received by the Secretary of Homeland Security (including assessments conducted under the *Implementing Recommendations of the 9/11 Commission Act of 2007*) across all transportation modes and realistic deadlines for addressing security needs associated with those assets referred to in subparagraph (A).

(C) The most appropriate, practical, and cost-effective means of defending those assets against threats to their security.

(D) A forward-looking strategic plan that sets forth the agreed upon roles and missions of Federal, State, regional, local, and tribal authorities and establishes mechanisms for encouraging cooperation and participation by private sector entities, including nonprofit employee labor organizations, in the implementation of such plan.

(E) A comprehensive delineation of prevention, response, and recovery responsibilities and issues regarding threatened and executed acts of terrorism within the United States and threatened and executed acts of terrorism outside the United States to the extent such acts affect United States transportation systems.

(F) A prioritization of research and development objectives that support transportation security needs, giving a higher priority to research and development directed toward protecting vital transportation assets. Transportation security research and development projects shall be based, to the extent practicable, on such prioritization. Nothing in the preceding sentence shall be construed to require the termination of any research or development project initiated by the Secretary of Homeland Security or the Secretary of Transportation before the date of enactment of the *Implementing Recommendations of the 9/11 Commission Act of 2007*.

(G) A 3- and 10-year budget for Federal transportation security programs that will achieve the priorities of the National Strategy for Transportation Security.

(H) Methods for linking the individual transportation modal security plans and the programs contained therein, and a plan for addressing the security needs of intermodal transportation.

(I) Transportation modal security plans described in paragraph (1)(B), including operational recovery plans to expedite, to the maximum extent practicable, the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident. These plans shall be coordinated with the resumption of trade protocols required under section 202 of the *SAFE Port Act* (6 U.S.C. 942) and the National Maritime Transportation Security Plan required under section 70103(a) of title 46.

(5) Priority Status.

(A) In general. The National Strategy for Transportation Security shall be the governing document for Federal transportation security efforts.

(B) Other plans and reports. The National Strategy for Transportation Security shall include, as an integral part or as an appendix:

(i) the current National Maritime Transportation Security Plan under section 70103 of title 46;

(ii) the report required by section 44938 of this title;

(iii) transportation modal security plans required under this section;

(iv) the transportation sector specific plan required under Homeland Security Presidential Directive-7; and
(v) any other transportation security plan or report that the Secretary of Homeland Security determines appropriate for inclusion.

The statute requires subsequent versions of the Strategy be submitted, "to appropriate congressional committees not less frequently than April 1 of each even-numbered year."[5] Further, in carrying out the responsibilities in the statute, the Secretary of Homeland Security, in coordination with the Secretary of Transportation, "shall consult, as appropriate, with Federal, State, and local agencies, tribal governments, private sector entities (including nonprofit employee labor organizations), institutions of higher learning, and other entities."[6]

[5] Id.
[6] Id.

II. Introduction

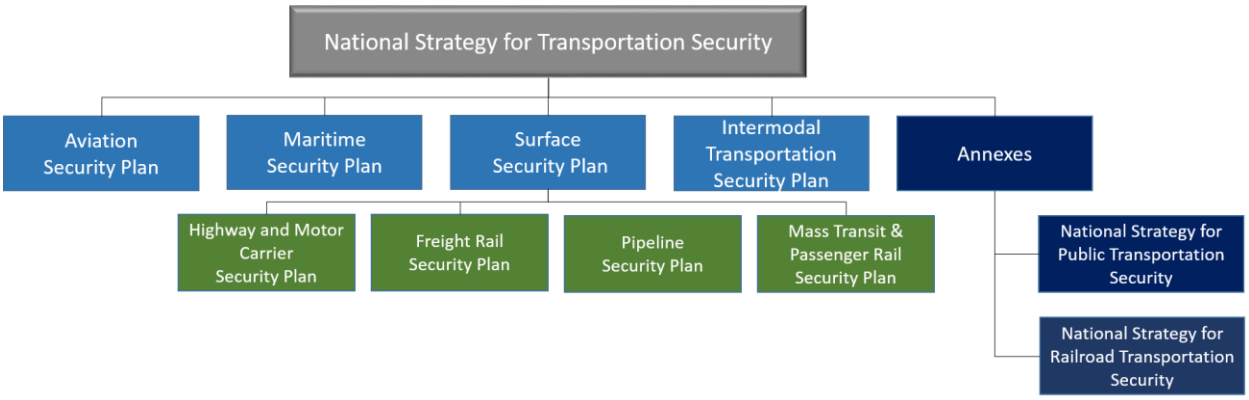
A. Purpose and Scope

The National Strategy for Transportation Security (the Strategy) fulfills a requirement of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA) to address security risks in the Nation's transportation systems.[7] The Strategy is developed jointly with the Department of Transportation (DOT) and submitted biennially on even numbered years.

The Strategy is a forward-looking plan that identifies and evaluates "transportation assets in the United States that, in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces…;" describes security risks to those assets; establishes risk-based priorities to manage the risks; and includes practical and cost-effective means to defend those assets.[8] The Strategy consists of a base plan and four security plans for aviation, maritime, surface, and intermodal systems. It also includes the National Strategy for Public Transportation Security (NSPTS) and National Strategy for Railroad Transportation Security (NSRTS) as annexes.[9]

While the Strategy is the "governing document for federal transportation security efforts," private sector cooperation and participation in carrying out their respective security responsibilities is vital for the security of the national transportation system.[10] The Strategy builds upon the demonstrated commitment of the transportation industries to continually advance security programs through the most appropriate, practical, and cost-effective means.

Figure 1: NSTS Modal Plans and Strategies



[7] Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458 (December 17, 2004).
[8] 49 U.S.C. § 114(s)(3).
[9] As required by Implementing the Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. 110-53 (August 3, 2007).
[10] 49 U.S.C. § 114(s)(5) and (6).

B. Guiding Principles

Four guiding principles provide an overarching framework for developing and implementing the Strategy.

Agile, Adaptable Security Posture

Security comes at a cost to individuals, companies, and governments. The Strategy uses the Sector's multiple layers of security to manage risks with a proper balance of resources while preserving the vitality of the transportation system. The risk management approach applies risk segmentation methods to adapt security processes for low risks while sustaining appropriate procedures for higher risks.

Partnerships

Understanding and achieving effective and efficient security of the Nation's transportation systems involves the whole community: industry, employees, vendors, support services, travelers, shippers, and all levels of government to include law enforcement. Academia, unions, and professional organizations contribute significantly to security awareness and readiness. Open and trusting relationships encourage an environment of coordinated and shared responsibilities. Effective partnerships foster the unity of effort essential to preserving the freedom of movement and vitality of commerce on which our Nation relies.

Privacy and Civil Rights

The activities undertaken by security authorities must be carefully considered to prevent violations of civil rights, unwarranted invasion of privacy, and undue restrictions of civil liberties. Security plans and activities must preserve the liberties and freedoms upon which our Nation was founded.

Accountability

The transportation security partners are accountable to the American people for implementing effective and efficient programs to manage transportation security risks, while promoting the legitimate movement of people and commerce. The Strategy provides outcome-based measures to indicate the Sector's progress in reducing risks; increasing awareness; and protecting privacy, civil rights, and civil liberties.

C. Strategic Environment

The strategic environment evolves as adversaries strive to circumvent security measures. New methods and tactics to develop and deploy dangerous weapons are frequently circulated on the Internet. The proliferation of new technologies, such as non-metallic weapons and Unmanned Aircraft Systems (UAS), challenge current detection and protection methods. Frequent risk assessments are needed to identify security gaps associated with new threats and technologies. This evolving threat environment places an emphasis on intelligence sharing and domain awareness for timely deployment of protection measures, coordination of security resources, and activation of responders. As innovative cyber technologies enter the marketplace, cybersecurity risks also evolve. A cyber-attack and its cascading effects could disrupt vital transportation-related services across all modes in areas such as ticketing, navigation, and Industrial Control Systems (ICS).

The strategic environment considers the threats of, vulnerabilities to, and potential consequences of a terrorist attack. Security planners should consider the nature of the strategic environment to identify and prioritize risks and to develop strategic security priorities to reduce those risks.

1) Assets to Be Protected

Transportation assets that must be protected from attack are the infrastructure and systems that support the mobility essential to our way of life, national security, and economic prosperity.[11] Assets and systems meeting the criteria for protection under the Strategy are identified in the modal security plans based on assessments of the threats of, vulnerabilities to, and consequences of a successful attack. In general, these assets and systems include: commercial aviation including airlines and airports; general aviation; public transportation systems serving major urban areas; air cargo systems; strategic and commercially important seaports and waterways; and highways, tracks, tunnels, bridges, and transmission pipelines sustaining vital corridors and supply chains.

2) Current Risk Environment

The current risk environment includes international and domestic terrorist threats to the Nation's transportation system. Since 9/11, two successful attacks at the Los Angeles International Airport and a number of disrupted plots and attacks across the country show that terrorists are persistent, dynamic, and adaptive.[12] The Strategy takes into consideration the evolving nature of terrorist threats and the challenges posed by a more dispersed and less visible enemy. To address this dynamic threat, the Strategy is

On January 6, 2017, a passenger arriving at the Fort Lauderdale-Hollywood, Florida International Airport retrieved a firearm from his checked baggage, loaded it in a restroom, and emerged shooting the first people he encountered, killing 5 and wounding 6.

[11] 49 U.S.C. § 114(s)(3)(A).
[12] https://www.tsa.gov/news/features/2015/11/01/remembrance-gerardo-i-hernandez.

risk-based and intelligence-driven and relies on the rapid exchange of actionable threat and security information across government and industry.

Transportation remains a primary target for terrorists. Terrorists may place explosive devices on persons or in cargo and baggage. More recently attacks have involved other types of lethal weapons. Terrorists acting alone or in small groups may use small arms, edged weapons, or chemical or biological weapons. Terrorist threats to transportation also include the potential for hijackings, attacks by stand-off weapons such as man-portable air-defense systems or rocket-propelled grenades or by radiological and nuclear weapons. Intermodal hubs such as airports and transit stations are particularly exposed to attacks due to open public areas, often crowded conditions, and limited escape routes.

Another ongoing security concern is the potential for individuals or small groups, radicalized or otherwise motivated, to attack transportation assets in the United States. Terrorist organizations openly incite sympathizers in the United States to support and commit acts of violence through terrorist messaging presented in videos, magazines, and online forums. The risk posed by homegrown terrorists is a challenge, based on their ability to plan and conduct attacks without detection. The same goes for insiders—those having trusted positions and access to sensitive information or locations—willing to commit malicious acts. Insiders may act independently or incite others to commit cyber or physical attacks.

International threats to transportation are predominantly associated with transnational terror organizations, such as al-Qa'ida and the Islamic State in Iraq and Syria. Overseas attacks indicate aviation, public transportation, over-the-road buses, and pipeline assets as likely targets. Increasingly, terrorist tactics involve single or small teams of adversaries striking soft targets where people are densely gathered. The Strategy accounts for these types of targets and attack methods in the United States.

3) Emerging Risk Environment

Emerging security risks arise from threats and tactics recognized after international attacks and by advances in adversary capabilities, both physical and cyber. The exponential proliferation of UAS and a demonstrated use of UAS to bomb battlefield targets in the Middle East raise the specter of such an attack domestically.[13] Terrorists continue to develop and deploy innovative concealment methods, as exemplified by the use of laptops to conceal explosives.

[13] UAS, commonly known as drones, are regulated by the Federal Aviation Administration (FAA). A final rule for small UAS became effective on August 29, 2016, which amends Title 14 of the Code of Federal Regulations Parts (21, 43, 61, 91, 101, 107, 119, 133, and 183) operation and Certification of Small Unmanned Aircraft Systems; Final Rule, 81 Fed. Reg. 42064 (June 28, 2016). A small UAS consists of a small unmanned aircraft (which, as defined by statute (Pub. L. 112-95, sec. 331(6)), is an unmanned aircraft weighing less than 55 pounds) and equipment necessary for the safe and efficient operation of that aircraft. FAA is statutorily prohibited from imposing new requirements on hobby/recreational UAS that meet all of the criteria specified in section 336 of Public Law 112-95.

Similarly, while vehicles have long been used by terrorists to deliver IEDs, the use of vehicles as a weapon to ram into crowds—as seen in the truck attacks in Nice, France; Berlin, Germany; and Barcelona and Cambrils, Spain— reveal an emerging threat encouraged by terrorist messaging.

Emerging threats include the potential for terrorists and other hostile forces to use cyber-attacks to disrupt transportation operations or sabotage networked systems. Owners and operators of transportation assets and systems have embraced the efficiency and functionality that electronic communications and automation provide and have incorporated technological components into nearly every aspect of day-to-day operations. This dependence on internet-connected devices for critical communications, financial transactions, reservations, ticketing (among other business functions), and ICS and Supervisory Control and Data Acquisition (SCADA) systems for remote operability, provides an increasingly complex set of cyber vulnerabilities that can be exploited by threat actors. Cyber adversaries will continue to develop capabilities and further refine their techniques to most effectively accomplish their goals. As transportation systems and assets become increasingly automated and connected, and adversaries' intents and capabilities change, the cyber risk will grow and evolve. While there have been few incidents of chemical and biological attacks domestically, due to the growing accessibility of the underlying technologies associated with the use of biological, chemical, and radiological agents as weapons, these threats also present a significant future risk.

On July 14, 2016, Bastille Day, in Nice, France, a Tunisian national living in France drove a large truck into a crowd of revelers resulting in the death of 86 people and injuring 434.

On December 19, 2016, a Tunisian national in Berlin, Germany, hijacked a commercial truck and plowed into crowds at a Christmas market killing 12 people and injuring 56.

On August 17 and 18, 2017, vehicles driven by Islamic State in Iraq and Syria (ISIS)-affiliated terrorists plowed into crowds in Barcelona and Cambrils, Spain, killing 17 and injuring over 120 people.

On October 31, 2017, a terrorist in a truck sped down a bike path in New York City taking the lives of 8 and injuring 12.

On December 11, 2017, a lone terrorist in a walkway at the New York City Port Authority Bus Terminal detonated an improvised explosive device (a crude pipe bomb) carried in the back pack he was wearing. The explosion injured five including the bomber.

D. Challenges

The challenges listed here are those factors, issues, or circumstances in the strategic environment that may render corrective actions less certain and favorable outcomes more difficult.

1) Uncertainty About Risks

Terrorist threats are unpredictable. Consequently, threat and vulnerability assessments often involve assumptions and subjective methods that introduce varying degrees of uncertainty into the assessment results. These uncertainties may raise doubts about the effectiveness of security actions and inhibit security investment decisions.

2) Resource and Budget Constraints

Sustaining a robust counterterrorism security posture requires significant resources and funding for physical security investments, planning, and recurring personnel training. Federal security grants complement state, local, tribal and territorial government efforts to design, develop, employ, and sustain security programs for eligible transportation systems operators and owners, and for law enforcement providers.

The 3- and 10-year budget for federal transportation security programs to achieve the priorities of the Strategy presents challenges for security managers. While the out-year budgets are informed by strategic planning, they are also a tool for policy implementation, accountability, and performance. The budgets will continue to be submitted through the established President's Budget process. The challenge is anticipating future security programming and aligning budget projections for transportation security across multiple government departments and agencies. For example, federal funding of transportation security is largely through grants managed by the Department of Homeland Security (DHS) Federal Emergency Management Agency (FEMA) and DOT. Projecting security funding for future grants—where safety and security are co-mingled across multiple agencies—is imprecise and unrealistic. To address this challenge, the Strategy contributes to departmental budgetary processes by applying multiple information sources (intelligence, risk assessments, and exercises) to determine priorities and capability gaps that influence resource allocation decisions and budget projections across federal agencies. The Strategy also supports out-year programming and budgeting by measuring the progress achieving the security outcomes for funded activities.

3) Performance Assessments

Measuring the effectiveness of security initiatives across multiple government jurisdictions and diverse industries presents challenges for resource managers. In a resource constrained fiscal environment, security program effectiveness should be evaluated based on meaningful assessments of the benefits of risk-reduction activities and their associated costs. This presents several challenges, including: 1) assessing baseline risk equitably across all transportation services and 2) assessing the effectiveness of specific initiatives. Even if reliable risk-reduction metrics are available in one mode, comparing them to another mode is often not feasible or possible. Transportation security partners should jointly consider outcome-based performance measures during program development and, to the extent practicable, apply assessment methodologies to inform decisions.

4) Resilience and System Recovery

A terrorist attack involving transportation assets and systems could have considerable long-term consequences on travel and commerce. The recovery of transportation services following an attack is dependent on the resilience of the systems and on the integrity of the infrastructure. Cascading impacts of an attack disrupting transportation could affect regional and local communities that depend on transportation assets such as key bridges or tunnels for work, school, or day-to-day needs. The national preparedness mission areas listed here span a continuum of capabilities that should be considered and coordinated among all jurisdictional elements contributing to resilient communities.

National Preparedness Goal
Five Mission Areas*

1. **Prevention**
2. **Protection**
3. **Mitigation**
4. **Response**
5. **Recovery**

*** FEMA, National Preparedness Goal 2015**

III. Mission, Vision, Strategic Goals, and Risk-Based Priorities

Mission: Secure the Nation's transportation system from acts of terrorism.

Vision: A secure and resilient transportation system, enabling travelers and goods to move freely without significant disruption of commerce or loss of civil liberties.

Figure 2: Development of Risk-Based Priorities

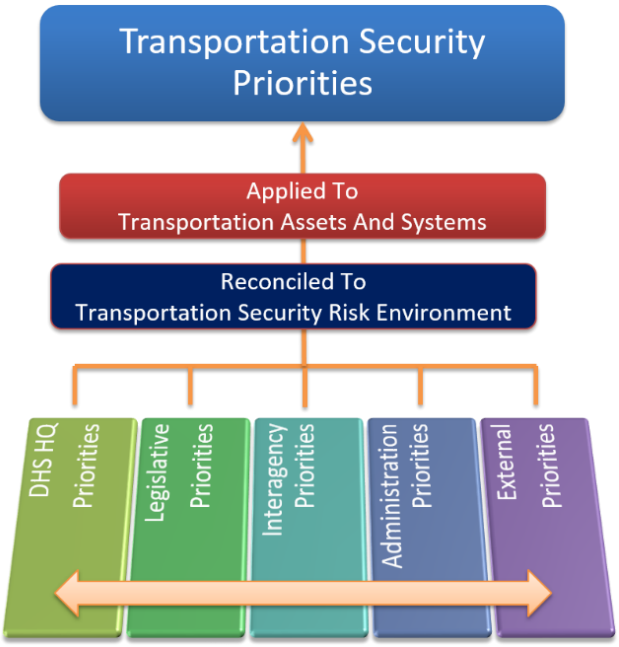


Figure 2 depicts the multiple sources used to understand the Nation's security priorities. Congressional, executive, other governmental, and industry security priorities are considered in the context of transportation system operations. Security risks to transportation systems are aligned with national security priorities and applied to the transportation assets and systems that must be protected from terrorist attacks. The transportation risk-based priorities inform security decisions about the types of activities government and industry modal security officials should pursue, independently and jointly, to address terrorism risks. The specific actions to implement the risk-based priorities provide a multi-layered defense and response posture that span the preparedness mission areas. These risk-based priorities are further developed in the modal security plans.

A. Goal 1: Manage Risks to Transportation Systems from Terrorist Attack and Enhance System Resilience

Security managers develop priorities to counter known risks and prepare for unforeseen risks. Managing risks involves deploying security countermeasures and enhancing system resilience. These activities help to narrow capability gaps and raise the security baseline.

Risk-Based Priority 1: Physical Security
Physical security includes the protective actions taken during asset construction and operations such as structural resilience, barriers, access controls, patrols, video surveillance, and alarms. Physical security measures should be developed to close gaps identified by risk assessments that consider threat, vulnerability, and consequence.

Risk-Based Priority 2: Weapons Detection Programs
Weapons detection programs are designed to prevent the introduction of weapons of mass destruction or other lethal weapons into transportation systems whether carried on a person, in baggage, or in cargo. Federal agencies, local law enforcement, local transit authorities, and private industry employ canines, behavioral detection methods, and a variety of sensor, screening, and advanced information technologies to reduce the possibility that dangerous items could be introduced into aviation, maritime, and surface transportation modes.

Insiders who combine advanced technological understanding with traditional espionage/terrorist skills have a significantly increased asymmetric capability to cause physical damage through cyber-means.

Source: National Risk Estimate: Risks to U.S. Critical Infrastructure from Insider Threat, December 2013, DHS National Protection and Program Directorate, Office of Cyber and Infrastructure Analysis.

Risk-Based Priority 3: Cybersecurity
Cybersecurity risks in transportation operations vary in vulnerabilities and consequences across the transportation modes. Commercially available tools enable threat actors to hack into business networks or Industrial Control Systems (ICS) to compromise the safety of transportation operations. The Strategy encourages system owners and operators to assess the threats to their cyber systems and to invest appropriately to secure them.

Risk-Based Priority 4: Preventing Terrorist Travel and Insider Threats
Preventing terrorist travel is a top priority. Insiders within the transportation workforce may, wittingly or unwittingly, facilitate terrorist activities. The Strategy emphasizes screening and vetting countermeasures such as biometric facial recognition, personnel security assessments, and credentialing programs to address these risks.

Risk-Based Priority 5: Preparedness
The Strategy recognizes that successful preparedness measures depend on well-trained and informed security personnel, frontline employees, first responders, law enforcement

officers, and other stakeholders at the Federal Government and state, local, tribal, and territorial (SLTT) government levels. The transportation community relies on close cooperation with emergency managers to enhance preparedness capabilities for responses to a variety of threats such as suicide bombers, terrorists, or other hostile forces through effective partnerships and practiced and coordinated operations. As appropriate, transportation system recovery planning and operations will conform to the resumption of trade protocols developed pursuant to section 202 of the SAFE Port Act.[14]

B. Goal 2: Enhance Effective Domain Awareness of Transportation Systems and Threats

> **"Risk management is not an end in and of itself, but rather a part of sound organizational practices that include planning, preparedness, program evaluation, process improvement, and budget priority development. The value of a risk management approach or strategy to decision makers is not in the promotion of a particular course of action, but rather in the ability to distinguish between various choices within the larger context."**
>
> ***Source: Risk Management Fundamentals: Homeland Security Risk Management Doctrine.***

Domain awareness is a key enabler for continuous risk identification and informed decision making. It is defined as "the observation of the operating domain (air, land, and maritime) and its baseline information."[15] Successful domain awareness improves the government's ability to share information at the appropriate classification level regarding current and emerging risks and threats to the homeland. Through domain awareness security personnel are better able to understand threats and to manage security risks within the scope of their functions and responsibilities.

Risk-Based Priority 1: Assessments

An initial step to managing terrorism risks across all modes is to understand how transportation assets, systems, and networks may be attacked. The intelligence community assesses current threats and other indicators to provide transportation owners and operators with timely and useful information to address and mitigate risks to their operations. Additional assessment of vulnerabilities and potential attack consequences enable security managers in government and industry to evaluate risks locally, regionally, and nationally. Recurrent assessments allow program managers to evaluate the effectiveness and efficiency of risk management efforts and to adjust programs accordingly.

Risk-Based Priority 2: Information Sharing

The information collected through assessments must be reliable, analyzed, and distributed efficiently and effectively to all responsible parties having the need to know. The

[14] 6 U.S.C. § 942.

[15] Air and Marine Operations Vision 2025, p. 12.

transportation system uses multiple processes to disseminate intelligence and security information. The processes, procedures, and network infrastructure used for timely access to classified and unclassified information must be exercised and evaluated frequently to ensure that accurate, pertinent information flows quickly to operators, government, public safety and security officials, and the public.

Risk-Based Priority 3: Situational Awareness, Common Operating Picture
Situational awareness is required to effectively coordinate operations across the five preparedness mission areas. The Federal Government supports the enhancement of technologies and data standards that facilitate a common operating picture for decision makers to access critical and time sensitive information.

Risk-Based Priority 4: Training
Training, including exercises and drills, teaches and hones proper security awareness and procedures. Training provides the foundation for physical and cybersecurity programs that effectively secure transportation assets, systems, and networks. Security training prepares transportation frontline employees and security professionals to deter, prevent, detect, and mitigate terrorist activities.

C. Goal 3: Safeguard Privacy, Civil Liberties, and Civil Rights; and the Freedom of Movement of People and Commerce

Managing risk, enhancing resilience, and effective domain awareness are contingent upon our ability to safeguard privacy, protect civil liberties, and ensure the freedom of movement of people and commerce.

Risk-Based Priority 1: Accelerated Screening of Low-Risk Passengers and Cargo
Accelerated screening of low-risk passengers and cargo improves the passenger experience and the efficiency of supply chain operations. Security officials apply technologies, data sources, and analytical methods to evaluate the risks associated with passengers and cargo and to make risk-based decisions on the necessary level of screening.

Risk-Based Priority 2: Protecting Civil Rights and Liberties during Screening
The security screening process must respect the unique personal circumstances of travelers and protect their civil rights and liberties. The Federal Government and contract security providers use modified security screening procedures for individuals with disabilities or medical conditions. These special procedures preserve security while accommodating the unique needs of the traveler.

Risk-Based Priority 3: Protecting Sensitive Information
The flow of passengers and goods in commerce requires the Federal Government and transportation companies to develop and process sensitive information including, but not limited to, classified national security information, personally identifiable information, and proprietary information. This information is managed largely through government

and industry cyber and data systems. Government and industry must apply strict security protocols to protect sensitive information.

IV. Performance

A. Assessing National Transportation Security Performance

Federal, SLTT, and industry partners work jointly to develop a performance assessment regimen to indicate progress in achieving priority security outcomes. Progress achieving security outcomes is determined by developing realistic deadlines, monitoring risk management activities and collecting data provided by government or transportation owners and operators who are responsible for implementing the activities.[16] Progress is reported annually to Congress on implementing the key activities in the Strategy, which is consistent with the progress reported annually in the President's Budget request.[17]

B. Security Program Performance Assessments

Assessments of transportation systems and infrastructure provide the primary means to understand the elements of risks, to develop risk-based priorities, and to determine progress addressing the risks. Security assessments can take many forms. Assessments may address different parts of risk—threats, vulnerabilities and consequences—or the total risk for specific assets or classes of assets. The Baseline Assessment for Security Enhancement (BASE) assessments and airport perimeter assessments, as well as the pipeline Critical Facility Security Reviews are examples of asset-specific assessments. Some assessments address regional or locality risks. DHS's Regional Resilience Assessment Program and the United States Coast Guard's (USCG) port security assessments are examples of geographically-oriented assessments. Risk assessments are also conducted to determine the effectiveness of specific security programs such as airport checkpoint screening or cargo anomaly detection programs. These various assessments collectively provide a picture of the security environment and the terrorism risks to inform decisions on risk-based priorities and remedial activities. While the transportation community relies on a wide variety of assessments, two provide the most comprehensive understanding of terrorism-related risks: (1) TSA's Transportation Systems Security Risk Assessment (TSSRA) and (2) the USCG Maritime Security Risk Analysis Model (MSRAM).

C. Strategic Performance Measures

The modal security plans provide metrics for key activities indicating the progress managing priority risks in each mode. Table 1 identifies the outcomes for the strategic priorities for each goal.

[16] 49 U.S.C. § 114(s)(3)(b).
[17] 49 U.S.C. § 114(s)(4)(c).

Table 1: Performance Measures

NSTS Goal	Risk-Based Priority	Outcome
Manage risks to transportation systems from terrorist attack and enhance system resilience.	• Physical Security • Weapon Detection Programs • Cybersecurity • Preventing Terrorist Travel and Insider Threat • Preparedness	Perimeters of sensitive transportation locations are not breached by terrorists. Critical infrastructure is hardened against terrorist attacks. Dangerous articles are not introduced into aviation. Weapons of Mass Destruction (WMDs) are not transported in containers. Chemical and biological threats are detected and neutralized. Terrorists are not able to travel by commercial aviation. Terrorists do not enter the United States. Transportation system employees in security sensitive positions are vetted to minimize security risks.
Enhance effective domain awareness of transportation systems and threats.	• Assessments • Information Sharing • Situational Awareness, Common Operating Procedures (COP) • Training	High-risk transportation assets and systems that must be protected are routinely assessed to determine progress-mitigating vulnerabilities. Transportation stakeholders are satisfied with intelligence-related and other security information shared. Emergency responders and stakeholders have satisfactory access to incident COP. Exercises and training include objectives to learn about and exercise domain awareness capabilities.
Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce.	• Accelerated Screening of Low-Risk Passengers and Cargo • Protecting Civil Rights and Liberties during Screening • Protecting Sensitive Information	Enrollment in TSA Pre✓® program and related programs is increased. Passenger screening time decreases. Policies are approved by officials responsible for protecting privacy, civil rights, and civil liberties. Enrollment in Customs-Trade Partnership Against Terrorism (C-TPAT) and related programs is increased. Cargo delays are minimized. Enhance the travel experience of persons with special needs.

V. Path Forward

The security responsibility of the Nation's transportation systems is shared among multiple jurisdictions at federal and SLTT levels and with public and private transportation owners and operators. Consequently, the management of security risks is dependent on interoperable communications systems, effective operational coordination, and timely information sharing among security partners. The Strategy envisions the following programmatic commitments to advance security of transportation assets and systems that must be protected from attack by terrorists or other hostile forces.

Risk Assessments and Security Planning: The security of the Nation's transportation systems is predicated on both a solid foundation of risk assessments and deliberate, prudent planning to manage priority risks. The two disciplines must coexist at corporate, municipal, state and federal levels to achieve coherent, cohesive, and cost efficient security solutions and to sustain preparedness to protect people, property, and our way of life.

Intelligence and Information Sharing: Information undergirds the security apparatus of the transportation community. To be responsive to the evolving risk environment, industry and government security professionals must hone current intelligence and information processes and procedures to ensure that information is exchanged and analyzed quickly, and that relevant, actionable information reaches all appropriate stakeholders in a timely manner.

Training and Exercises: Security professionals, law enforcement officials, employees and management, and first responders must be able to work together effectively during a crisis. The layered approach to security preparedness involves multiple organizations of federal, state and local government agencies whose rapid and coordinated actions will be essential to protect people and property. The Nation's transportation-service providers must maintain a well-trained workforce that is able to recognize, report, and respond appropriately to threats and to work effectively with responders during incidents. Initial and recurrent investment in security training and exercises will be a priority for the transportation community to develop and sustain interoperability through each phase of security preparedness: prevention, protection, mitigation, response, and recovery.

Supply Chain Security: Virtually every segment of our society depends on transportation services in one way or another for delivery of raw materials, products, food, medicines, and household goods. The efficiency and effectiveness of these supply chains are dependent, in large measure, on reliable delivery of goods over transportation systems and through intermodal connections and transshipment points. Transportation security officials should develop methodologies to incorporate the transportation elements of supply chains in future risk assessments and planning.

Enhanced Infrastructure Resilience: Infrastructure is the backbone of transportation systems. The Nation's seaports, airports, air navigation services, waterways, roads, rail track, bridges, tunnels, and pipelines are the physical by-ways for the movement of people and commerce. The state of repair of transportation infrastructure is an important aspect of the system's resilience. Reliable transportation infrastructure is a key to providing mobility and freedom of movement

and to sustaining effective supply chains for the Nation's manufacturing, refining, and commercial sectors.

Research and Development: While seeking to manage transportation security risk, security managers must continually strive to minimize impacts of security initiatives on the free movement of people and commerce. Research and development provide the means by which security initiatives can be examined to determine gaps in delivering effective, risk-based security solutions and to preserve, to the greatest extent practicable, the security and freedom of movement of people and commerce. Federal entities will continue to seek technologies and procedures that will enhance the detection of dangerous articles—particularly non-metallic weapons, innovatively concealed explosives, and chemical and biological agents—introduced in to the transportation system.

R&D priorities, not in prioritized order, are:

- Weapons of mass destruction, explosives, and intrusion detection and identification;
- High throughput threat detection;
- Behavior detection and biometric identification;
- Freight tamper prevention and detection;
- Blast mitigation;
- Remote disruption of attack;
- System resiliency and recovery technologies and procedures; and
- Interoperable information systems.

VI. Transportation Operational Recovery Planning

Mobility is essential to our way of life and a key factor in the economic vitality of the Nation. It is also a crucial component of emergency responses to disasters or attacks. Consequently, the Federal Government, states, communities, and transportation service providers plan and prepare for response and recovery from any event that disrupts transportation. Congress required DHS to include operational recovery plans in the modal security plans of the Strategy. The modal operational recovery plans provide protocols for the government planners and transportation company owners and operators to consider when developing transportation recovery plans.

DOT's Recovery Resource Guide: A Transportation Stakeholder Guide to Recovery[18] links transportation recovery processes with the principles found in the National Preparedness System (NPS), the National Response Framework (NRF), and the National Disaster Recovery Framework (NDRF). While these plans address the recovery of transportation systems generally, specific operational recovery protocols for the modes are provided in the modal security plans, attached to the Strategy as appendices.

Because most response and recovery actions begin, and are managed, at the local level, community involvement in the recovery planning is essential. States, regions, and communities plan for transportation recovery in concert with other aspects of transportation planning. DOT offers detailed guidance and protocols for transportation recovery planning on its Disaster Recovery website.[19] Additionally, DOT provides planning support to Metropolitan Planning Organizations in urban locations or Transportation Management Areas, as mandated by law. These organizations plan for all aspects of transportation operations and infrastructure projects, including response and recovery from disasters.

[18] https://www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE_Final%20Version_ 08-27-2014.pdf. Accessed May 4, 2017.
[19] https://www.transportation.gov/disaster-recovery. Accessed May 4, 2017.

Appendix A: 2018 Aviation Security Plan

Homeland Security

Transportation Security Administration

2018 Aviation Security Plan

I. Introduction

A. Overview

The 2018 Aviation Security Plan addresses the security of the Aviation Transportation System (ATS) through the four main components of the mode: commercial airlines, commercial airports, general aviation, and air cargo.[20] Within these modal components, a myriad of aviation support functions and activities provide services that require access to airport facilities and aircraft. Aircraft repair facilities, airport concessions, fuel services, ground maintenance and repair services, and food and drink vendors exemplify the extended community included in the aviation mode. Security for this extended aviation domain depends on effective partnerships and communication among governments—federal, SLTT, international—and industry stakeholders, including aircraft owners and operators, airport operators, shippers, industry associations, and passengers.

The ATS is vitally important to U.S. prosperity and freedom; disruption of the critical infrastructure elements in the aviation domain could create ripple effects throughout the entire system. Terrorists regularly consider the ATS and its components as targets for attack.

The Aviation Security Plan implements the presidential directive for aviation security policy to continue the enhancement of U.S. homeland and national security by protecting the United States and its interests from threats in the aviation domain.[21,22] It also provides a strategic approach to securing the aviation domain from terrorist attacks and advances the strategic goals of the Strategy by identifying objectives and activities.

1) Modal Profile

Aviation assets and systems that need to be protected in the interest of national security and commerce from attack by terrorists include: the air traffic control system, federalized domestic airports, foreign airports serving as the last-points-of departure for the United States, commercial airliners and cargo aircraft operating in the United States, general aviation aircraft, airports operating under TSA's Security Programs, air cargo industry, and flight schools.[23]

[20] The term "Aviation Transportation System" is defined as "U.S. airspace, all manned and unmanned aircraft operating in that airspace, all U.S. aviation operators, airports, airfields, air navigation services, and related infrastructure, and all aviation-related industry."
[21] National Security Policy Directive-47/Homeland Security Policy Directive-16.
[22] The term "Aviation Domain" is defined as "the global airspace, including domestic, international, and foreign airspace, as well as all manned and unmanned aircraft operating, and people and cargo present in that airspace, and all aviation-related infrastructures." National Strategy for Aviation Security (NSAS), 2007.
[23] See TSA approved Airport Security Program.

The risk management strategies address physical, human, and cyber elements of aviation activities and their supporting services, as necessary to protect life and property and to prevent disruption of the ATS.

The components in Table 2 identify the main sub-modal aviation communities and the organizational approach to security planning and programming.

Table 2: Components of the Aviation Mode

Air Cargo	Air cargo includes property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. The air cargo security operations serving the United States are made up of over 300 domestic and foreign air carriers, and over 4,000 indirect air carriers.
Commercial Airlines	Commercial airlines are those that engage in regularly scheduled passenger service or public charter operations including domestic aircraft operators and foreign air carriers flying within, from, to, or over the United States.
Commercial Airports	Commercial airports are defined as public airports that have at least 2,500 passenger boardings per year and have scheduled passenger service.[24] There are approximately 450 airports in the United States that have airport security programs. TSA assesses certain non-U.S. airports to satisfy statutory requirements as well as to determine compliance with International Civil Aviation Organization Standards and Recommended Practices.
General Aviation	General aviation encompasses a wide variety of civil aircraft operations other than state aircraft operations, or scheduled commercial aircraft operations. It includes all types of aircraft and supports diverse industries and activities, including private-use aircraft, business jet, and emergency medical helicopter operations. General aviation aircraft use approximately 19,300 private and public airports, heliports, and landing strips in the United States, of which more than 5,100 are public-use airports including commercial airports described above.
Flight Schools	Flight schools include any pilot school, flight-training center, air-carrier flight-training facility, flight instructor, or any other person or entity that provides instruction in the operation of any aircraft or aircraft simulator.
Repair Stations	Foreign and domestic repair stations inspect, repair, replace or overhaul aviation products and articles including airframes, engines, propellers and radios among others.

2) Risk Profile

The risk profile for the aviation mode of transportation includes threats from domestic actors, but is dominated by transnational terrorism.[25] The greatest threat to aviation security remains explosives, especially non-metallic Improvised Explosive Devices (IEDs). New and emerging

[24] Title 49 USC 47102(7).
[25] Risk Profiles and Scenarios sources include Transportation Systems Security Risk Assessment (TSSRA) and TSA aviation assessments.

technologies such as Non-Traditional Aviation Technology (NTAT) provide opportunities for terrorists to attack aviation targets in ways that are difficult to detect.

International and Domestic Terrorists: Terrorist attacks frequently involve IEDs deployed on a person, in cargo or baggage, or in a vehicle to attack transportation assets. Commercial aircraft may be used as a weapon of mass destruction or may transport radiological or nuclear materials in cargo. Travelers at intermodal aviation and transit venues are exposed to other types of attacks due to open and congested public areas. The public areas allow attackers access to populated assembly areas for ticketing, baggage pick-up, or screening. Terrorists acting alone or in small units may gain access to crowded terminals to perpetrate attacks using explosives, small arms, edged weapons, or chemical or biological weapons. An on-going security concern is the potential for individuals or small groups inside the United States who are radicalized or otherwise motivated to violence to attack transportation assets. Terrorist organizations openly incite—through videos, magazines, and online forums—sympathizers in the United States to support and commit acts of violence. The risk posed by these homegrown terrorists is enhanced by their ability to plan and conduct attacks with less risk of detection. Returning foreign fighters create substantial risks to the homeland when they travel to another country to link up with terrorists and return with a terrorist purpose.

Trusted Insiders: Individuals having trusted positions and access to sensitive information or locations and who are willing to commit malicious acts are often more difficult to detect. Insiders may facilitate cyber or physical attacks by others or act independently.

Non-Traditional Aviation Technology: Unmanned Aircraft Systems (UAS), often referred to as drones, used for business, research, and recreation are opening a broad new avenue for delivery of weapons by terrorists. From both a recreational and commercial perspective, UAS proliferation will continue to increase and their technology will evolve. While most of the operators of these systems are pursuing legitimate activity, the risk of an irresponsible or malicious actor using the system is increasing. UAS are easily obtained and could be used to deliver a lethal payload of explosives or chemical, biological, or radiological/nuclear agents with little opportunity for interdiction. UAS can be launched from anywhere and may not be detected on radar, therefore, normal means of detecting the threat may not work for a UAS attack. While the impact of an individual UAS attack might be small, a coordinated attack by several UAS could have a major impact.

The risk profiles listed in Table 3, informed by TSSRA and other intelligence analyses provide the basis for risk-based aviation security priorities.

Table 3: Aviation Risk Profiles

Air Cargo Risk Profile	Air cargo risks are magnified by the vast number and diversity of shippers, cargo handlers, and carriers in the global supply chain. Air cargo is transported on a wide range of aircraft—from large express consignment carriers that operate complex sorting operations at major hubs to small regional carriers that move high-value cargo or serve rural areas. The presence of cargo shipments on passenger aircraft increases the security risk level of the cargo.
Commercial Airlines Risk Profile	The risk of terrorists attacking or using commercial aircraft includes threats of hijacking, the introduction of explosives or other weapons into the aircraft, and attacks using standoff weapons such as man-portable air-defense systems especially at international last points-of-departure airports and particularly in high threat regions. While security measures have significantly reduced aviation risks, aircraft-related security risks remain elevated due to persistent attempts by terrorists to thwart security measures.
Commercial Airports Risk Profile	Commercial airports are multi-modal hubs characterized by efficient and convenient access to arrival and departure areas of the terminals. The greatest risks for airports are related to attacks in publicly accessible areas. IEDs may be introduced in baggage, on persons, or by vehicles. Secure areas of airports, though tightly controlled, are vulnerable to forcible intrusion by individuals or small tactical units that could breach checkpoints or perimeter barriers. Terrorist attacks may also be facilitated by insiders, wittingly or unwittingly, providing information or access needed to execute an attack.
General Aviation Risk Profile	The terrorist threats to general aviation operations and facilities are understandably similar to those for commercial aviation and federalized airports. General aviation facilities are generally considered to have a lesser risk of terrorist attack than commercial aviation facilities due to the smaller size and limited volume of travelers. General aviation aircraft are vulnerable to being used by terrorists for travel, logistics, or operations. Moreover, as vulnerabilities associated with commercial passenger operations are mitigated, it is believed that terrorists may view general aviation as more vulnerable and thus attractive targets.

B. Risk-Based Priorities

Risk-Based priorities are program areas that manage risks. Aviation analysts review data from security assessments and inspections, exercises, and incident reports to identify vulnerabilities and develop risk management strategies. The following risk-based priorities for the aviation mode are derived from analyses of congressional or executive direction, legislation, threat intelligence, risk assessments, and gap analysis.

Physical Security: Physical security includes the protective actions taken during asset construction and operations such as structural resilience, barriers, access controls, patrols, surveillance, and alarms. Physical security measures should be developed to close vulnerability gaps identified by security inspections, threat assessments, and consequence analyses.

Screening Technology: Screening technology detects and prevents the introduction of weapons or other lethal agents into transportation venues whether carried on a person, in baggage, or in cargo. Federal agencies and private industry employ a variety of screening and advance information technologies to mitigate the risk of introducing dangerous items into aviation, maritime, and surface transportation systems.

Training: Training, including exercises and drills, teaches and hones proper security awareness and procedures. Training provides the foundation for successful physical and cybersecurity programs that effectively secure transportation assets, systems, and networks. Security training prepares transportation employees at all levels and security professionals to deter, prevent, detect, and mitigate terrorist activities.

Information Sharing: The information collected through assessments must be reliable, analyzed, and distributed efficiently and effectively to all users. The transportation system uses multiple processes to disseminate intelligence and security information. The processes, procedures, and network infrastructure used for timely access to classified and unclassified information must be exercised and evaluated frequently. This will ensure that accurate, pertinent information flows quickly to aircraft and airport operators, government, public safety and security officials, and the public.

Preventing Terrorist Travel and Insider Threat: Preventing terrorist travel remains a top priority. The Strategy emphasizes countermeasures to improve screening and vetting capabilities such as automated biometric matching against watch lists, personnel security assessments, and credentialing programs. Additionally, terrorist attacks may also be facilitated by insiders within the transportation workforce including workers employed by transportation companies, on-site vendors, or contract personnel who, wittingly or unwittingly, supply information needed to execute an attack.

Protecting Civil Rights and Liberties during Screening: The security screening process must respect the unique personal circumstances of travelers and protect their civil rights and liberties. The Federal Government and private-security service providers use modified security screening procedures for individuals with disabilities or medical conditions. These special procedures preserve security while accommodating the unique needs of the traveler.

Accelerated Screening of Low-Risk Passengers and Cargo: Transportation efficiency is an important aspect of global supply chains and the passenger experience. However, unrestricted mobility presents unacceptable risks in the present threat environment. Security officials apply technologies, data sources, and analytical methods to evaluate the risks associated with travelers and cargo and to make risk-based decisions on the necessary level of screening.

Protecting Sensitive Information: The flow of passengers and goods in commerce requires the Federal Government and transportation companies to handle large amounts of sensitive information including classified national security, personal, and proprietary information. Information is managed through multiple government and industry data systems. Government and industry are committed to strict security protocols for these data systems to protect private, personal, and sensitive data as well as the integrity of the computer networks that process it.

II. Objectives, Activities, and Measuring Progress

The 2018 Aviation Security Plan's goals and objectives reflect the risk-based priorities. Table 4 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national aviation security.

Table 4: Aviation Security Goals

NSTS Goal 1	**Manage risks to ATS from terrorist attacks and enhance system resilience**
Objective 1: **Improve physical and cybersecurity of domestic aviation critical infrastructure.**	**Activity 1:** Increase the number of aviation workers that require a fingerprint based Criminal History Records Check (CHRC) and have unescorted access to non-public areas of airports who receive perpetual vetting of their criminal history through Rap Back (DHS/TSA/Federal Bureau of Investigation (FBI), and industry).[26] **Outcome:** Reduction in insider threat vulnerability by aviation workers. **Performance Measurement:** Percentage of aviation workers that require a CHRC and have unescorted access to non-public areas of airports that receive perpetual vetting through Rap Back. --- **Activity 2:** Assess cybersecurity in commercial aircraft. **Outcome:** Identify and mitigate cyber vulnerabilities affecting safe operations of commercial aircraft. **Performance Measurement:** Percentage of organizations that have implemented at least one aviation cybersecurity enhancement after receiving a vulnerability assessment or survey (National Protection and Program Directorate).
Objective 2: **Improve capabilities to prevent, protect, mitigate, respond to, and recover from terrorist attacks throughout the aviation community.**	**Activity 1:** Continually expand training for frontline employees to strengthen technical skills to identify, deter, prevent, and respond to threats to the homeland (DHS/TSA and industry). **Outcome:** Prohibited items are not introduced into the aviation system. **Performance Measurement:** Improvement in detection rates for covert testing and annual proficiency reviews.

[26] The Rap Back service allows authorized agencies to receive notification of activity on individuals who hold positions of trust (e.g. school teachers, daycare workers) or who are under criminal justice supervision or investigation, thus eliminating the need for repeated background checks on a person from the same applicant agency. https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi, Accessed February 1, 2018.

NSTS Goal 1	Manage risks to the ATS from terrorist attacks and enhance system resilience
Objective 3: **Enhance international aviation security risk management strategies.**	**Activity 1:** Conduct outreach to facilitate the use of international best practices and procedures (Department of Justice/FBI, DHS/U.S. Customs and Border Protection (CBP)/TSA, DOT/FAA, and Department of State). **Outcome:** International policies support U.S./DHS objectives of raising the baseline of global aviation security. **Performance Measurement:** Percentage of foreign airports that take action to raise the baseline of global aviation security by addressing vulnerabilities identified by intelligence information. Actions could include, the installation of new technology (i.e. Computed Tomography), the use of canine teams authorized by the host government, and/or collaboration with DHS towards becoming preclearance airports. --- **Activity 2:** Assess compliance with security measures for international inbound passengers, cargo, and baggage (DHS/CBP/TSA). **Outcome:** To identify compliance with TSA required security standards for passengers, baggage, and cargo transported to the United States. **Performance Measurement:** Percentage of international inspections and assessments indicating that TSA-required security standards for passengers, cargo including submission of Air Cargo Advanced Screening (ACAS) information, and baggage, are being met. --- **Activity 3:** Scan international inbound air cargo shipments entering the U. S. to detect radiological or nuclear threats (DHS/CBP/Countering Weapons of Mass Destruction (CWMD) Office.). **Outcome:** Reduction of the risk of illicit radiological or nuclear agents entering the United States. **Performance Measurement:** Percent of international air cargo, including special express commercial services cargo and mail, that passes through radiation detection systems upon entering the nation at air ports of entry.
Objective 4: **Increase security technology capability to respond to known and emerging threats.**	**Activity 1:** Leveraging TSA work to harmonize standards internationally, improve aviation industry stakeholder participation in the Research and Development (R&D) process for threat detection and screening capabilities (DOT, DHS/TSA/Science and Technology Directorate, R&D community, and industry) **Outcome:** Increased aviation industry stakeholder participation in processes to identify security capability gaps and develop solutions on a global scale. **Performance Measurement:** Improved aviation industry stakeholder participation in the Research and Development process to harmonize global detection and screening capabilities.

NSTS Goal 2	Enhance effective aviation domain awareness of transportation systems and threats[27]
Objective 1: **Improve quality in the sharing of intelligence information and products for government, industry, and public awareness.**	**Activity 1:** Enhance the customer satisfaction of intelligence products to security partners. **Outcome:** Improve the quality of intelligence products for customers. **Performance Measurement:** Percentage of customer satisfaction surveys indicating high quality and timeliness of intelligence products (TSA/Office of Intelligence and Analysis, industry).

NSTS Goal 3	Safeguard privacy, civil liberties, civil rights, and the freedom of movement of people and commerce
Objective 1: **Reduce the impact of security policies and activities to privacy, civil rights, and civil liberties.**	**Activity 1:** Include the Office of Civil Rights and Liberties, Ombudsman and Traveler Engagement (OCRL) in the coordination process for new security policies involving the screening of individuals/passengers. **Outcome:** Security policies are drafted in such a manner that they minimize the impact on privacy, civil right, and civil liberties of individuals subject to enhanced screening. **Performance Measurement:** Increase in security policies coordinated and approved by OCRL.
Objective 2: **Apply risk-based security approach to supply chain and passengers.**	**Activity 1:** Screen all inbound air cargo shipments to resolve security risks of high-risk cargo, including high-risk cargo identified by ACAS, prior to loading for shipment to or upon arrival in the United States. **Outcome:** Enhance freedom of movement of low-risk cargo. **Performance Measurement:** Percentage of cargo by value imported to the United States by participants in CBP trade partnership program (CBP). --- **Activity 2:** Provide expedited aviation security screening for trusted travelers. **Outcome:** Enhance legitimate traveler experience. **Performance Measurement:** Percentage of daily passengers receiving expedited screening based on assessed low risk and continue to explore options to garner greater efficiencies in TSA Pre✓® and Global Entry.

[27] NSAS, 2017.

III. Aviation Operational Recovery Plan

Transportation services are an essential part of our daily lives and the economic vitality of communities. Operational recovery plans for the transportation modes establish protocols for government, communities, and industry to restore transportation services following a disruption as quickly as possible.

The Aviation Transportation System Recovery Plan is one of seven supporting plans of the NSAS. It "defines a suite of strategies to mitigate the operational and economic effects of an attack in the Air Domain, as well as measures that will enable the Aviation Transportation System and other affected critical government and private sector aviation-related elements to recover from such an attack as rapidly as possible."[28]

In concert with the federal recovery plans, airport and air carrier security programs are required under federal regulations to have emergency response procedures and contingency plans in place.

Title 49 Code of Federal Regulations (CFR) 1542.307 requires airports to have a security program to address emergency response procedures for incidents or threats and to review their emergency response procedures on an annual basis.

Title 49 CFR 1544.301 requires aircraft operators to have a current contingency plan in place and participate in airport-sponsored exercises for incident response.

[28] Aviation Transportation System Recovery Plan, 2007.

Appendix B: 2018 Maritime Security Plan

Homeland Security

Transportation Security Administration

2018 Maritime Security Plan

I. Introduction

A. Overview

Our Nation's maritime critical infrastructure continues to face complex and evolving challenges. Maritime risks stem from a mix of naturally occurring and man-made hazards and threats, including terrorist attacks, both domestic and international, and cyber threats. The 2018 Maritime Security Plan addresses the security of maritime assets that must be protected from terrorist attacks in the interest of national security and commerce.

The goals in preventing or responding to terrorist attacks, or in recovering from natural or marine disasters are the same: to save lives, preserve property, minimize disruption to the Marine Transportation System (MTS) and the maritime community, and protect the environment. The public and private sector develop collaborative protocols for prevention of, protection against, response to, and recovery from incidents.

The security of the MTS relies on the engagement of the maritime community. Federal entities, SLTT agencies, waterway users, industry, foreign governments, and international operators are vital partners in the collaborative effort to secure the system and ensure its resilience.

1) Modal Profile

The MTS in the United States is a geographically, physically, and operationally diverse network of maritime and shore side operations consisting of 25,000 miles of navigable channels, 238 locks at 192 locations, and over 3,700 marine terminals. Waterborne cargo and associated activities contribute more than $742 billion annually to the U.S. Gross Domestic Product and sustains more than 13 million jobs.[29] Over 75 percent (by weight) of international trade enters or leaves the United States by ship.[30] Enhancing the security of and protecting U.S. interests in the maritime domain are national security policy objectives administered by USCG with TSA and CBP support. This includes prevention of terrorist attacks in the maritime domain, and enhancement of U.S. national security and homeland security by protecting U.S. critical transportation infrastructure, borders, ports, waterways, and coastal approaches in the maritime domain. Maritime elements of the vital global supply chains serving the Nation are among the critical assets and systems that must be protected. CBP and OCWMD are principal partners in maritime supply chain security. Goods entering the United States from or destined to international points are subject to screening and inspection for compliance with international and

[29] U. S. Chamber of Commerce Policy Statement on Marine Transportation, 08-05-2012. https://www.uschamber.com/issue-brief/marine-transportation, Accessed August 30, 2017.
[30] Federal Highway Administration, Freight Facts and Figures 2013. Available at http://ops.fhwa.dot.gov/freight/freight_analysis/nat_freight_stats/docs/13factsfigures/figure2_05.htm#metric. Accessed December 3, 2015.

domestic trade and security protocols. TSA administers the Transportation Worker Identification Credential Program for transportation personnel that need access to secure areas of port facilities. Federal, state, and local authorities in the ports coordinate their various mission responsibilities to provide security layers to manage physical, cyber, and personnel risks. These risk management efforts are complemented by funds provided by the Federal Emergency Management Agency through the Port Security Grant Program.

2) Risk Profile

Terrorism Risk: A successful terrorist attack in the U.S. maritime domain, particularly in a heavily populated port area involving especially hazardous cargo, could have devastating effects, including the potential deaths of thousands of people, adverse economic impacts, and the disruption of domestic and international trade. Assessments indicate maritime terrorism will remain a concern as commerce increases and terrorists improve capabilities or alter attack methods. International terrorists may seek access to the United States through ports and waterways. Consequently, the homeland security enterprise will need to focus on detecting suspicious activity in the maritime domain adjacent to and within U.S. borders.

> **Weapons of Mass Destruction:** The extreme consequences of a WMD event make it a significant risk. A comprehensive set of threat identification and detection capabilities is required to reduce the threat of their transfer. Vessels less than 300 gross tons (considered small vessels) could be targeted by terrorists or saboteurs as opportunities to smuggle dangerous weapons, including WMD, into the United States.
>
> **Terrorist Transfer:** The risk of transfer of terrorists by a vessel of any size into the United States is a serious concern. The deadly December 2008 attacks in Mumbai, India, highlighted the threats posed by small vessels used to convey terrorists into or through any nation's maritime domain. The probability of such an attack may increase with the expected growth in the movement of passengers, vessels, and hazardous cargo.

Small Vessel Terror Attack: Millions of small commercial and recreational vessels operate on U.S. waterways. Vessels less than 300 gross tons are not required to carry electronic identification devices, make advance notices of arrival, or otherwise alert authorities to their whereabouts; thus they constitute a major maritime domain awareness gap. Consequently, a more likely threat may be the use of a waterborne IED on a small vessel to attack a ship or waterfront facility. In addition, small vessels may be used to conduct standoff attacks. In 2008, terrorists used inflatable motorboats to stealthily land on the waterfront near Mumbai, India and then moved inland to conduct multiple attacks over a four-day period killing 164 and wounding at least 308. Pirates in many parts of the world have used small speedboats armed with rocket-propelled grenades and automatic weapons to attack yachts, cruise ships, freighters, and tankers and to hold cargo, ships, and crew hostage.

Cyber Risk: Both cyber exploitation by malicious actors, including terrorists, as well as unintentional incidents due to operator error or accidental software/hardware failures, pose a risk to maritime transportation. Maritime operations rely on cyber-based technologies for communications, navigation, positioning, tracking, cargo handling and stowage, and shipboard

control systems. These systems are often networked with shore-based systems. Cyber-attacks targeting the systems on which vessels and port operations rely are unlikely to cause significant disruption of national or regional maritime operations due to the overall resilience of the commercial port and maritime industries. However, localized impacts such as port delays and interrupted delivery schedules could occur.

Especially Hazardous Cargo Release: Especially hazardous cargos are transported, transferred, and stored in numerous ports and waterways, particularly the Gulf Coast region and the Western Rivers.[31] Due to their chemical and physical properties, their release in the MTS could threaten nearby populations, cause significant damage to the environment, and disrupt commerce.

B. Risk-Based Priorities

The USCG Maritime Security Risk Analysis Model: MSRAM is a terrorism risk management tool and process deployed to USCG analysts across the country, enabling them to perform a detailed risk analysis for their area of responsibility. The results of this process are used to support a variety of risk management decisions at the strategic, operational, and tactical levels within and across U.S. ports. The model helps industry and government risk managers and operational decision makers to understand the distribution of risks across the Nation's ports, the risks within a port, and asset-specific risks. For example, risk profiles within a port support operational planning and resource allocation. The MSRAM Program Office also collaborates with CWMD in risk assessment modeling for the evaluation of strategies for the Global Nuclear Detection Architecture. In addition, USCG's National Maritime Strategic Risk Assessment uses enterprise data, subject matter expert judgments, and analyses of data from other models to provide a comprehensive view of the maritime risk environment over a 5 to 8-year time horizon.

The maritime risk-based priorities are:

- Conduct domestic and international port-level risk assessments;
- Implement risk-based security planning and operations to reduce the terrorism risk;
- Increase enforcement of international maritime security regimes;
- Enhance maritime domain awareness;
- Conduct maritime security and response operations; and
- Enhance cyber safety, security, and resilience for MTS owners/operators.

[31] "Especially hazardous cargo means anhydrous ammonia, ammonium nitrate, chlorine, liquefied natural gas, liquefied petroleum gas, and any other substance, material, or group or class of material, in a particular amount and form that the Secretary [of Homeland Security] determines by regulation poses a significant risk of creating transportation security incident while being transported in maritime commerce." 46 U.S.C. §70103(e)(2)(B).

II. Objectives, Activities, and Measuring Progress

The Maritime Security Plan's goals and objectives reflect the risk-based priorities. Table 5 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national maritime security.

Table 5: Maritime Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist attack and enhance system resilience**
Objective 1: **Use risk-based security planning and operations to reduce the terrorism risk to the Marine Transportation System.**	**Activity 1:** Improve compliance at Maritime Transportation Security Act facilities through risk-based adjustment of enforcement operations tempo (USCG). **Outcome:** Reduce vulnerabilities at high-risk maritime facilities. **Performance Measurement:** Security compliance rate for high-risk maritime facilities (DHS 2015-2017 Annual Progress Report (APR), Appendix A, p. 55). --- **Activity 2:** Improve interoperability of federal and SLTT response teams in Maritime and Security Response Operations (MSRO) (USCG). **Outcome:** Reduce risks of terrorist planning and precursor activities. **Performance Measurement:** Percentage change from year to year in port-level deployments of MSRO. --- **Activity 3:** Employ MSRAM and other risk assessment and analysis tools to refine the estimates of MSRO activities' risk-reduction benefits, and use these estimates to inform the execution of MSRO activities in U.S. ports (USCG). **Outcome:** Improve port risk evaluations to reduce port vulnerabilities. **Performance Measurement:** Percentage change in port risk estimates from MSRAM modeling. --- **Activity 4:** Identify and assess high-risk inbound cargo (CBP). **Outcome:** Reduce risk of terrorists exploiting the global supply chain. **Performance Measurement:** Percentage of inbound cargo identified by CBP as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry (DHS 15-17 APR, App A, p. 60).

NSTS Goal 1	Manage risks to transportation systems from terrorist attack and enhance system resilience
Objective 2: **Reduce security vulnerabilities and improve preparedness throughout the Marine Transportation System.**	**Activity 1:** Expand cybersecurity protections in all segments of the MTS using the National Institute of Standards and Technology Framework (USCG). **Outcome:** Reduce risk of a malware or cyber-attack disrupting maritime commerce. **Performance Measurement:** Percentage of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey (DHS 2015-2017 APR, Appendix A, p. 29). --- **Activity 2:** Improve International Ship and Port Facility Security Code implementation in foreign ports that send ships to the United States (USCG). **Outcomes:** Improve security (identify risks) at foreign ports serving ships destined for the United States. **Performance Measurement:** Percentage of planned foreign port and reciprocal visits completed. --- **Activity 3:** Evaluate containerized cargo for illicit radiological or nuclear material (DHS/CWMD). **Outcome:** Reduce the risk of illicit radiological or nuclear material entering the United States. **Performance Measurement:** Percentage of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry (DHS 2015-2017 APR, Appendix A, p. 8) (CBP/CWMD).

NSTS Goal 2:	Enhance effective domain awareness of MTS and threats
Objective 1: **Improve the security, resilience, and regulatory (federal/SLTT) information sharing process throughout the Marine Transportation System community.**	**Activity 1:** Enhance resilience of cyber systems through exercises, guidance, and assessments (USCG). **Outcome:** Improve awareness of and action to reduce the risk of cyber threats or malware. **Performance Measurement:** Percentage of organizations that have implemented at least one cybersecurity enhancement after receiving a cybersecurity vulnerability assessment or survey (DHS 15-17 APR, Appendix A, p. 29).

NSTS Goal 2:	Enhance effective domain awareness of MTS and threats
Objective 2: **Improve Marine Transportation System stakeholder participation in the risk management process for security and resilience prioritization and programming.**	**Activity 2:** Improve effectiveness of port exercise programs by designing exercise objectives and events based on analysis of MSRAM risk data (USCG). **Outcome:** Improve risk-based design of port exercises. **Performance Measurement:** Percentage of security exercises that include using MSRAM data.

NSTS Goal 3:	Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce
Objective 1: **Collaborate with international partners to increase the reliability of the global supply chain.**	**Activity 1:** Apply risk segmentation methods to evaluate cargo for expeditious clearance (CBP). **Outcome:** Secure and expedite trade. **Performance Measurement:** Percentage of cargo by value imported to the United States by participants in CBP trade partnership programs (DHS 15-17 APR, App A, p. 57).

III. Maritime Operational Recovery Plan

Transportation services are essential to our way of life and economic prosperity. Disruptions can have debilitating effects on communities, businesses, regions, and the Nation. Operational recovery plans for the transportation modes establish protocols for government, communities, and industry to restore transportation services as quickly as possible following a disruption.

Homeland Security Presidential Directive 13, Maritime Security Policy, directed DHS to develop a National Strategy for Maritime Security. Eight additional supporting plans were required to address, in greater detail, certain aspects of maritime security including recovery from disruptions.[32] The Maritime Infrastructure Recovery Plan (MIRP), published in April 2006, contains procedures for recovery management and provides mechanisms for national, regional, and local decision-makers to set priorities for redirecting commerce, a primary means of restoring domestic cargo flow.[33] Decision-making affecting the nation's entire MTS draws on both domestic and international resources for recovery and relies on comprehensive maritime domain information to inform operational decisions about alternate ports or routes for shipping and cargo destinations. Consequently, the MIRP focuses on restoring maritime transportation capabilities (i.e., restoration of passenger and cargo flow), expediting the recovery of trade, and minimizing the impact of a disruption on the U.S. economy.

[32] The eight supporting plans for the National Strategy for Maritime Security are: 1) National Plan to Achieve Maritime Domain Awareness, 2) Global Maritime Intelligence Integration Plan, 3) Maritime Operational Threat Response Plan, 4) International Outreach and Coordination Strategy, 5) Maritime Infrastructure Recovery Plan, 6) Maritime Transportation System Security Recommendations, 7) Maritime Commerce Security Plan, and 8) Domestic Outreach Plan.

[33] https://www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf. Accessed May 4, 2017.

Appendix C: 2018 Surface Security Plan

Homeland Security

Transportation Security Administration

2018 Surface Security Plan

Surface Transportation Overview

The 2018 Surface Security Plan fulfills a requirement established by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to address the threats, vulnerabilities, and consequences for transportation assets that could be at risk from attack or disruption by terrorists or other hostile forces.[34] The Surface Security Plan includes the modal plans for Mass Transit and Passenger Rail (MTPR), Freight Rail, Highway and Motor Carrier (HMC), and Pipeline.

Table 6: Surface Transportation Modes

Mass Transit and Passenger Rail	Includes transit buses, trolleys, monorails, heavy rail (subway), light rail, streetcars, and commuter and intercity passenger railroads. There are approximately 6,800 local transit providers serving more than 28 million riders daily and more than 10 billion riders annually. Amtrak and Alaska Railroad provide the Nation's only long-distance passenger rail; Amtrak carried 31.3 million passengers in FY 2016.
Freight Rail	Includes the 138,000-mile network of railroads, with more than 1.6 million freight cars and nearly 27,000 locomotives in service. The network is also made up of more than 76,000 bridges and 800 railroad tunnels. The network handles almost 28 million carloads of vital raw materials and finished products each year.
Highway and Motor Carrier	Includes bridges, major tunnels, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, and school buses travelling on over 4 million miles of roadway, approximately 612,000 bridges, and 473 tunnels.
Pipeline	Includes more than 2.7 million miles of pipeline in the United States network transporting nearly all of the natural gas and approximately 70% of hazardous liquids, including crude and refined petroleum. Above-ground assets of note include compressor stations and pumping stations.

The surface transportation modes determine their risk-based priorities using a common set of security themes that provide a foundation for a broad span of risk-based activities in each mode: planning, training, exercises, information sharing, infrastructure protection, risk-reduction, and community outreach. While the means to address risks may vary by mode, the strategic approach is to create a collaborative environment for government and industry to plan for and implement security programs, procedures, and processes. Each mode customizes these themes to its unique security needs.

[34] 49 U.S.C. § 114(s).

Mass Transit and Passenger Rail Security Plan

I. Introduction

A. Overview

The MTPR Security Plan operationalizes the strategies identified in the National Strategy for Public Transportation Security (NSPTS) and National Strategy for Railroad Transportation Security (NSRTS), and has been collaboratively developed by government officials and industry stakeholders to enhance and sustain capabilities for protection of the Nation's mass transit and passenger rail systems from terrorist attack.[35] This plan meets the modal security planning requirements established by IRTPA.[36]

1) Modal Profile

The mass transit and passenger rail mode includes public and private transportation agencies and companies. Federal and SLTT governments authorize, regulate, and provide financial support—in varying degrees—to many public and private mass transit and passenger rail operations. Reducing security vulnerabilities in transit and passenger rail operations, critical assets, and infrastructure is a collaborative and shared responsibility between TSA and mass transit and passenger rail owners and operators. Owners and operators have the primary responsibility for the safety and security of their infrastructure, systems, and passengers. As such, to best support MTPR owners and operators with their security needs, TSA focuses its efforts on periodic system assessments, voluntary operator compliance with industry standards, accurate and timely exchange of intelligence and information, and facilitating security drills and exercises. TSA also provides operational support in the form of providing trained explosives detection canines to MTPR systems, and random baggage screening support. While security initiatives outlined in this plan extend to all mass transit and passenger rail operators, this plan focuses on those agencies that are identified as higher-risk.

TSA and its government partners like the Federal Emergency Management Agency strive to advance mass transit and passenger rail modal security through collaborative efforts to establish national security priorities, identify capability gaps, and provide Transit and Intercity Passenger Rail Security Grant Program funding, which is administered by the Federal Emergency Management Agency (FEMA), and other resources to address risks. TSA also works closely with mass transit and passenger rail systems to identify and assess vulnerabilities of the higher-risk mass transit and passenger rail systems both for operational activities and critical infrastructure assets of national importance, and works with agencies to identify resources, including grants, and to implement programs that buy-down risk and mitigate identified vulnerabilities.

---

[35] The NSPTS and the NSRTS are at Annexes I & II.
[36] 49 U.S.C. § 114(s).

2) Risk Profile

Public transportation systems face significant challenges in making their systems secure. Certain characteristics make them both vulnerable and difficult to secure. For example, the high ridership of some systems makes them attractive targets for terrorists but also makes certain security measures, such as airport style checkpoints, impractical. Other methods and technologies protect travelers from risks associated with: high concentrations of travelers; multiple, open access points; and limited exit lanes. Risks increase in urban areas due to the convergence of multiple transportation systems and the higher densities of travelers at intermodal terminals. These systems typically have fixed publicly accessible transit schedules. The open access to transit conveyances and the difficulties associated with securing high volumes of passenger traffic present inherent vulnerabilities for hostile actions by lone actors or terrorist teams. Elevated risks are also associated with underground and underwater tunnels, common to many mass transit and passenger rail routes.

Recent attacks overseas and online terrorist messaging confirm that public transportation systems continue to be high-value targets for terrorists. While a limited number of terrorist attacks or attempted attacks have occurred against mass transit and passenger rail assets in the United States since 9/11, public transportation systems are common targets overseas. The majority of the overseas attacks targeted buses, railroad tracks, mass transit trains, and bus stations. Terrorist tactics and techniques used overseas could easily be used to conduct similar attacks in the United States.

3) Risk Scenarios

The risk scenarios inform the selection of activities to implement the risk-based priorities and address security vulnerabilities.[37]

- Armed assault and active-shooter situations;
- WMDs including chemical/biological attacks;
- Cyber-attack;
- IEDs aboard a train/in a station/on a platform;
- Insider threat; and
- Sabotage of infrastructure causing derailment.

B. Risk-Based Priorities

The risk-based priorities identified in the NSPTS and NSRTS provide the programmatic focus for the MTPR Security Plan's activities to reduce terrorism risks identified in the preceding Risk Profile and Risk Scenario sections.

The seven risk-based priorities in no particular order are:

[37] Transportation Sector Security Risk Assessment 5.0 (2016).

- Security planning;
- Security training;
- Security exercises;
- Critical infrastructure protection;
- Operational detection and deterrence;
- Intelligence and security information sharing; and
- Community outreach.

II. Objectives, Activities, and Measuring Progress

The MTPR goals and objectives reflect the risk-based priorities. Table 7 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national MTPR security.

Table 7: MTPR Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist attacks and enhance system resilience**
Objective 1 Security Planning: **Reduce the risks associated with a terrorist attack on MTPR systems through security plans that address critical infrastructure protection, operational practices (to detect and deter), and cybersecurity.**	**Activity 1:** Develop security plans, review, and update based on available information (Industry/DHS/TSA). **Outcome:** Improvement of industry security plans and security planning for both physical and cyber security through incorporation of best practices and lessons learned into existing security plans. **Performance Measurement:** Percentage of high-risk transit agencies participating in Baseline Assessment for Security Enhancement(BASE) assessments achieving a positive rating for security planning.
Objective 2 Security Training: **Conduct training of employees to identify, prevent, respond, and recover from a terrorist attack.**	**Activity 1:** Improve the current state of the Nation's most critical MTPR systems security training program through the incorporation of best practices and lessons learned into existing training plans (Industry/DHS/TSA). **Outcome:** Improve capability of industry employees to identify, prevent, respond and recover from a physical and/or cyber terrorist attack. **Performance Measurement:** Percentage of high-risk transit agencies participating in BASE assessments achieving a positive rating for security training.
Objective 3 Security Exercises: **Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.**	**Activity 1:** MTPR systems participate in exercises to evaluate the preparedness for, response to, and recovery from physical and cyber security incidents (Industry/DHS/TSA). **Outcome:** MTPR systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents. **Performance Measurement:** Percentage of high-risk transit agencies participating in BASE assessments achieving a positive rating for security exercises including TSA's I-STEP exercises.

NSTS Goa1 2	Enhance effective domain awareness of transportation systems and threats
Objective 4 Intelligence and Information Sharing: **Maintain and enhance mechanisms for information and intelligence sharing between the MTPR industry and government.**	**Activity 1:** Provide timely and relevant information and intelligence to enhance industry's domain awareness (DHS/TSA). **Outcome:** Improve domain awareness through timely delivery of relevant intelligence and information products for MTPR industry to implement mitigation strategies to reduce risk. **Performance Measurement:** Trend of timely distribution of time sensitive intelligence products.
Objective 5 Community Outreach: **Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with MTPR systems.**	**Activity 1:** Promote MTPR security awareness in communities surrounding critical MTPR assets and systems (DHS/TSA). **Outcome:** MTPR industry, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt MTPR operations and endanger the community. **Performance Measurement:** Percentage of high-risk transit agencies participating in BASE assessments achieving a positive rating for public awareness and emergency preparedness programs.

NSTS Goal 3	Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce
Objective 1 Security Planning and Training: **Protect civil liberties and the freedom of movement of people and commerce.**	**Activity 1:** Develop policy pursuant to applicable privacy and civil liberties and civil rights laws, regulations and policies (DHS/TSA). **Outcome:** Conformity with applicable laws. Maintaining freedom of movement of people and commerce. **Performance Measurement:** Percentage of policies cleared for compliance through TSA's OCRL.

III. MTPR Operational Recovery Plan

Transportation services are essential to our way of life and for economic prosperity. Disruptions can have debilitating effects on communities, businesses, regions, and the Nation. Operational recovery plans establish protocols for government, communities, and industry to restore transportation services as quickly as possible following a disruption.

Mass transit operational recovery planning occurs at federal, state, local, tribal, and industry levels. Basic guidance for transit system recovery from disruptions is provided on the Department of Transportation's (DOT's) disaster recovery website: https://www.transportation.gov/disaster-recovery. The guidance encourages transit service operators to plan ahead for disaster recovery and to develop relationships within their communities for anticipated resource requirements. The transit system recovery plans should integrate with local government recovery plans and strategies.

For disruptions resulting from large-scale or national disasters, transit systems and local government plans should be compatible with the principles and protocols for recovery operations described in the National Response Framework, the National Disaster Recovery Framework and state disaster plans.[38] Transportation plans prepared to meet federal requirements by Municipal Planning Organizations or similar organizations may also address transportation system recovery protocols that should be considered in transit system recovery planning.

Due to the unique circumstances of transit infrastructure and operations in each jurisdiction, transit recovery plans may vary substantially in specific detail. However, fundamental principles provided on DOT's disaster recovery website should be applied in transit system planning and exercise. Effective coordination and integration of all entities contributing to disaster response and recovery are necessary for expeditious recovery of essential public transportation services.

[38] Information on the Frameworks is provided on the FEMA website: https://www.fema.gov/national-planning-frameworks.

Freight Rail Security Plan

I. Introduction

A. Overview

The 2018 Freight Rail Security Plan, which operationalizes the strategies identified in the NSRTS, has been collaboratively developed by government officials and industry stakeholders to enhance and sustain capabilities for protection of the Nation's railroad system from terrorist attack. This plan meets the modal security planning requirements established by IRTPA of 2004.[39]

1) Modal Profile

The U.S. freight rail network consists of approximately 138,000 rail miles operated by seven Class I railroads—railroads with operating revenues of $475.5 million or more, 21 regional railroads, and 546 local (aka Short Line) railroads. U.S. freight railroads are private companies responsible for their own infrastructure maintenance and improvement projects to ensure security, safety, and a state of good repair. Railroads are subject to safety and security regulations, as authorized by Congress, related to specific cargos and operations. The Federal Government shares intelligence, security information, and best practices with the freight rail community and, on a periodic basis, conducts security assessments and facilitates exercises to examine threats and vulnerabilities of the freight rail network.

While security initiatives apply broadly to railroad operators, the 2018 Freight Rail Security Plan focuses on those railroad assets and operational areas that have the greatest risk of attack and thus need to be protected in the interest of national security. Critical asset categories in the freight rail network include bridges, tunnels, train dispatching centers, data centers, and train control systems.

Cooperative and independent company security initiatives enable the railroads to assess their own risks and refine operational, business continuity, and security plans. TSA and its government partners strive to advance security through collaborative efforts to establish national security priorities, identify vulnerabilities and capability gaps, and reduce risks.

2) Risk Profile

The freight rail network is a vital part of the national economy, playing a key role in the global supply chain for both raw materials and finished goods. Freight rail is an important carrier for intermodal containers, often delivering imported goods to inland ports and domestic products across regions and states. As such, many sectors of the economy depend on freight railroads as a primary transporter, whether for commodities necessary to their operations, or for products and

[39] 49 U.S.C. § 114(s).

resources bound for domestic and international markets. Disruptions to critical nodes of the national rail network could have adverse impacts on efficient flows of the supply chains serving multiple sectors.

Freight railroads also "host" passenger rail operations over a significant portion of the network. Segments of the freight rail network where passenger and commuter rail share the same tracks are exposed to additional risk of attacks directed at passenger operations. Other security priorities in freight rail include the movement of Rail Security-Sensitive Materials (RSSM) shipments through densely populated areas and High Threat Urban Areas (HTUAs) and cyber risks to freight rail operations that could adversely affect critical supply chains of food, fuel, and other raw materials essential for critical industries.

3) Risk Scenarios

Freight rail attack scenarios are focused on attacks causing mass casualties or causing disruption of the rail network and inform the selection of activities to implement the risk-based priorities and countermeasures to address security vulnerabilities.[40,41]

- Sabotage to infrastructure causing the derailment of passenger trains operating on freight rail tracks;
- IEDs or Vehicle Borne Improvised Explosive Devices (VBIEDs) causing the catastrophic release of hazardous rail cargos and/or damage to critical infrastructure;
- Simple attacks using small arms or IEDs; and
- Insider threat.

B. Risk-Based Priorities

Freight rail's risk-based priorities identified in the National Strategy for Railroad Transportation Security provide the focus for defining activities to reduce terrorism risks to railroad operations.

The seven risk-based priorities are:

- Security planning;
- Security training;
- Security exercises;
- Critical infrastructure protection;
- Operational detection and deterrence;
- Intelligence and security information sharing; and
- Community outreach.

[40] Transportation Sector Security Risk Assessment 5.0 (2016).
[41] 2016 Freight Rail Modal Threat Assessment (TSA Office of Intelligence and Analysis).

II. Objectives, Activities, and Measuring Progress

The 2018 Freight Rail Security Plan's goals and objectives reflect the risk-based priorities. Table 8 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national freight rail security.

Table 8: Freight Rail Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist attacks and enhance system resilience**
Objective 1 Security Planning: **Reduce the risks associated with terrorist attacks on freight railroads through security plans that address critical infrastructure protection, operational practices (to detect and deter), and cybersecurity.**	**Activity 1:** Develop security plans, review, and update based on available information (Industry/DHS/TSA). **Outcome:** Improvement of railroad security plans and security planning through incorporation of best practices and lessons learned into existing security plans. **Performance Measurement:** Railroads that transport RSSM in HTUAs will implement a security plan and review or revise it during the reporting period.
Objective 2 Security Training: **Conduct training of frontline employees to identify, prevent, and respond to a terrorist attack.**	**Activity 1:** Improve freight railroad security training programs through the incorporation of best practices and lessons learned into existing training curriculum (Industry/DHS/TSA). **Outcome:** Improved capability of the freight railroad employees to identify, prevent, and respond to a physical and/or cyber terrorist attack. **Performance Measurement:** Railroads that transport RSSM in HTUAs will report the number of frontline employees receiving security-related training during the reporting period.
Objective 3 Security Exercises: **Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.**	**Activity 1:** Railroads participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents (Industry/DOT/DHS/TSA). **Outcome:** Railroads and public safety agencies are better prepared to respond and recover effectively in the event of physical and cyber security incidents. **Performance Measurement:** Railroads that transport RSSM in HTUAs will report the number and type of security-related exercises that the railroads conducted or participated in during the reporting period.

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
Objective 4 Intelligence and Information Sharing: **Maintain and enhance mechanisms for information and intelligence sharing between the freight rail industry and government.**	**Activity 1:** Provide timely and relevant information and intelligence to enhance freight railroads' domain awareness (DHS/TSA). **Outcome:** Improved domain awareness through timely delivery of relevant intelligence and information products to enable freight rail carriers to implement mitigation strategies to reduce risk. **Performance Measurement:** Positive trend in timely distribution of time sensitive intelligence products.
Objective 5 Community Outreach: **Engage with first responders and the public to provide awareness of security concerns associated with railroad operations in order to promote situational security awareness and preparedness.**	**Activity 1:** Promote freight railroad security awareness in communities surrounding critical freight assets and systems (DHS/TSA). **Outcome:** Freight railroads, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt freight operations and endanger the community. **Performance Measurement:** Railroads that transport RSSM in HTUAs report the number of engagements or activities related to enhancing the security preparedness with public safety, law enforcement, or emergency management organizations.

NSTS Goal 3	Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce
Objective 1 Security Planning and Training: **Protect civil liberties and the freedom of movement of people and commerce.**	**Activity 1:** Develop policy pursuant to applicable privacy and civil liberties and civil rights laws, regulations and policies (DHS/TSA). **Outcome:** Conformity with applicable laws. Maintaining freedom of movement of people and commerce. **Performance Measurement:** Percentage of policies cleared for compliance through TSA's OCRL.

III. Freight Rail Operational Recovery Plan

Railroads serve vital supply chains that enable our way of life and our economic prosperity. Disruptions of rail lines occur frequently due to human and natural causes and can have debilitating effects on communities, businesses, regions, and the Nation. Consequently, railroad companies integrate recovery practices into operational plans. Operational recovery plans provide the means to integrate the recovery responsibilities of railroad owners and operators with local authorities for rapid restoration of rail service and minimize traffic disruptions.

Federal recovery protocols are provided by DOT's disaster recovery website, the National Transportation Recovery Strategy, and the Recovery Resource Guide: A Transportation Stakeholder Guide to Recovery.[42,43,44] These sources integrate the transportation system recovery with information about other federal disaster plans and programs such as the National Preparedness System, the National Response Framework, the National Disaster Recovery Framework, and funding resources to restore the highway networks to pre-disaster conditions.[45,46]

Railroad disruptions involving emergency response are managed at the local level so community involvement in transportation recovery planning and preparedness is critical. State and community protocols to restore transportation services may be interspersed in emergency management plans or in regional plans undertaken by multi-jurisdictional organizations responsible for all transportation planning.

[42] https://www.transportation.gov/disaster-recovery. Accessed May 4, 2017.
[43] https://www.transportation.gov/sites/dot.gov/files/docs/DISASTER-RECOVERY-national-transportation-recovery-strategy-Final.pdf. Accessed May 4, 2017.
[44] https://www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE_Final%20-Version_08-27-2014.pdf. Accessed May 4, 2017.
[45] https://www.fema.gov/national-preparedness-system. Accessed February 9, 2018.
[46] https://www.fema.gov/national-planning-frameworks. Accessed February 9, 2018.

Highway and Motor Carrier Security Plan

I. Introduction

A. Overview

The Highway and Motor Carrier (HMC) Security Plan establishes risk-based priorities to protect the Nation's roads, bridges, tunnels, cargo carriers, and travelers from attacks or use by terrorists. The strategic priorities addressed in this plan represent the collaborative view of the mode's owners, operators, and Federal Government agencies. These organizations coordinate security initiatives and achieve strategic efficiency through alignment or consolidation of federal, state, and private programs. This plan recognizes some risks are persistent due to the dynamic nature of business ownership and uncertainty associated with the adversaries' intentions and capabilities. The priorities described in this plan narrow security gaps that otherwise provide opportunities for terrorists. This plan meets the legislative requirements established by the IRTPA.[47]

1) Modal Profile

The highway system—comprising commercial trucking, highway transportation infrastructure, over-the-road bus (OTRB), and school bus operations—is an integral part of the Nation's economy and way of life. More than 604 million passengers travel on OTRB and motor coaches annually and more than 25 million schoolchildren ride more than 480,000 school buses each day.[48,49] Efficient freedom of movement of commercial trucks carrying raw materials and finished products in the Nation's supply chains is essential for domestic and global markets.

Highway and motor carrier assets, systems, and services that need to be protected in the interest of national security and commerce include operations and infrastructure necessary to deliver raw materials and products of the Nation's vital supply chains. This plan also recognizes as a national transportation security priority, the protection of school bus and motor coach operations that provide passenger services, which underpin our way of life in every community across the nation.

2) Risk Profile

Highway transportation infrastructure provides the framework to move people and goods safely and securely.[50] Bridges, causeways, and underground and underwater tunnels are important

[47] 49 U.S.C. § 114(s).
[48] American Bus Association Foundation's annual Motorcoach Census (2015) (https://www.buses.org). Accessed January 1, 2018.
[49] American School Bus Council (http://www.americanschoolbuscouncil.org/about-asbc/mission-statement). Accessed May 4, 2017.
[50] American Bus Association, American School Bus Council, American Trucking Association, and the Department of Transportation, Federal Highway Way Administration.

infrastructure nodes in highway systems requiring special security considerations. While the Nation's highways are resilient, large-scale disruptions of these systems may adversely affect the Nation's economy and global markets. Terrorists may attack highway assets—structures, trucks, or buses—directly or use vehicles to deploy explosives or other weapons to attack targets. Confined areas, such as inside buses and bus terminals, also present potentially attractive targets for releasing chemical and/or biological agents, as those pathogens would have maximum impact and effect in confined spaces where egress options are limited or non-existent, and ventilation can also be a challenge. Highway transportation infrastructure is potentially vulnerable to disruption by terrorists with cascading consequences for supply chains and other sectors. An example of infrastructure vulnerability that can disrupt supply chains occurred on March 30, 2017, when a fire involving materials stored under a bridge spanning Interstate 85, south of Atlanta, caused the bridge to collapse, closing north and south bound lanes. Detours and alternative routing sent ripples through supply chain networks and rail and bus transit services serving Atlanta with secondary impacts on multiple sectors.

3) Risk Scenarios

The HMC attack scenarios inform the development of risk-based priority planning. [51,52] These attack scenarios include:

- Attacks using Improvised Explosive Devices (IED) or Vehicle-borne Improvised Explosive Devices (VBIED) on critical infrastructure such as bridges or tunnels;
- Small arms or IED attacks on passenger or school buses;
- A direct attack using a truck or vehicle loaded with explosives or toxic materials as a weapon against people or property;
- Use of a vehicle as a kinetic weapon (ramming) to cause loss of life or significant damage to critical infrastructure;
- Insider threat; and
- Intentional contamination of food products during bulk transportation.

B. Risk-Based Priorities

HMC risk-based priorities provide the programmatic focus for activities to reduce terrorism risks identified in the preceding Risk Profile and Risk Scenario sections.

The seven risk-based priorities are:

- Security planning;
- Security training;
- Security exercises;
- Critical infrastructure protection;
- Operational detection and deterrence;

[51] Transportation Sector Security Risk Assessment 5.0 (2016).
[52] 2016 Highway and Motor Carrier Modal Threat Assessment (TSA Office of Intelligence and Analysis).

- Intelligence and security information sharing; and
- Community outreach.

II. Objectives, Activities, and Measuring Progress

The HMC Security Plan's goals and objectives reflect the risk-based priorities. Table 9 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national HMC security.

Table 9: HMC Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist attacks and enhance system resilience**
Objective 1 Security Planning: **Reduce the risks from a terrorist attack on HMC systems through security plans that address critical infrastructure protection, operational practices (to detect and deter) and cybersecurity.**	**Activity 1:** Develop security plans, review, and update based on available information (Industry/DHS/TSA). **Outcome:** Improvement of industry security plans and security planning through incorporation of best practices and lessons learned into existing security plans. **Performance Measurement:** Percentage of HMC systems participating in the Baseline Assessment for Security Enhancement (BASE) achieving a positive rating for security planning.
Objective 2 Security Training: **Conduct training of employees to identify, prevent, respond to and recover from a terrorist attack.**	**Activity 1:** Improve the current state of the most critical HMC systems security training program through the incorporation of best practices and lessons learned into existing training plans (Industry/DHS/TSA). **Outcome:** Improved capability of the industry employees to identify, prevent, respond to, and recover from a terrorist attack. **Performance Measurement:** Percentage of HMC systems participating in BASE assessments achieving a positive rating for security training.
Objective 3 Security Exercises: **Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.**	**Activity 1:** HMC systems participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents (Industry/DHS/TSA). **Outcome:** HMC systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents. **Performance Measurement:** Percentage of HMC systems participating in BASE assessments achieving a positive rating for security exercises.

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
Objective 4 Intelligence and Information Sharing: **Maintain and enhance mechanisms for information and intelligence sharing between the HMC industry and government.**	**Activity 1:** Provide timely and relevant information and intelligence to enhance industry's domain awareness (DHS/TSA). **Outcome:** Improved domain awareness through timely delivery of relevant intelligence and information products for HMC industry to implement mitigation strategies to reduce risk. **Performance Measurement:** Positive trend in timely distribution of time sensitive intelligence products.
Objective 5 Community Outreach: **Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with HMC systems.**	**Activity 1:** Promote HMC security awareness in communities surrounding critical HMC assets and systems (DHS/TSA) **Outcome:** HMC industry, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt HMC operations and endanger the community. **Performance Measurement:** Percentage of highway and motor carrier systems participating in BASE assessments achieving a positive rating for sharing security related information or best practices.

NSTS Goal 3	Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce
Objective 1 Security Planning and Training: **Protect civil liberties and the freedom of movement of people and commerce.**	**Activity 1:** Develop policy pursuant to applicable privacy and civil liberties and civil rights laws, regulations and policies (DHS/TSA). **Outcome:** Conformity with applicable laws. Maintaining freedom of movement of people and commerce. **Performance Measurement:** Percentage of policies cleared for compliance through TSA's OCRL.

III. HMC Operational Recovery Plan

Highway roads, bridges, and tunnels are in many respects the arteries of mobility that enable our way of life and our economic prosperity. Disruptions of roads and highways can have debilitating effects on communities, businesses, regions, and the Nation. Operational recovery plans provide protocols to guide the state and local planning for rapid restoration of traffic and commerce.

Federal highway recovery protocols are provided by DOT's disaster recovery website, the National Transportation Recovery Strategy (NTRS), and the Recovery Resource Guide: A Transportation Stakeholder Guide to Recovery.[53,54,55] These sources integrate the transportation system recovery with information about other federal disaster plans and programs such as the National Preparedness System, the National Response Framework, the National Disaster Recovery Framework, and funding resources to restore the highway networks to pre-disaster conditions.[56,57]

Most response and recovery actions begin and are managed at the local level, so community involvement in transportation recovery planning and preparedness is critical. State and community protocols to quickly restore traffic flows may be interspersed in traffic and emergency management plans or in regional plans undertaken by multi-jurisdictional organizations responsible for all transportation planning.

[53] https://www.transportation.gov/disaster-recovery. Accessed May 4, 2017.
[54] https://www.transportation.gov/sites/dot.gov/files/docs/DISASTER-RECOVERY-national-transportation-recovery-strategy-Final.pdf. Accessed May 4, 2017.
[55] https://www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE FINAL%20Version 08-27-2014.pdf. Accessed May 4, 2017.
[56] https://www.fema.gov/national-preparedness-system. Accessed February 9, 2018.
[57] https://www.fema.gov/national-planning-frameworks. Accessed February 9, 2018.

Pipeline Security Plan

I. Introduction

A. Overview

The Pipeline Security Plan describes national pipeline security goals, objectives, and activities developed with government and industry stakeholders to reduce risks to nationally significant pipeline systems. This plan provides an operational approach for the pipeline community, which secures the Nation's pipeline transportation systems from terrorist attacks and enhances system resilience.

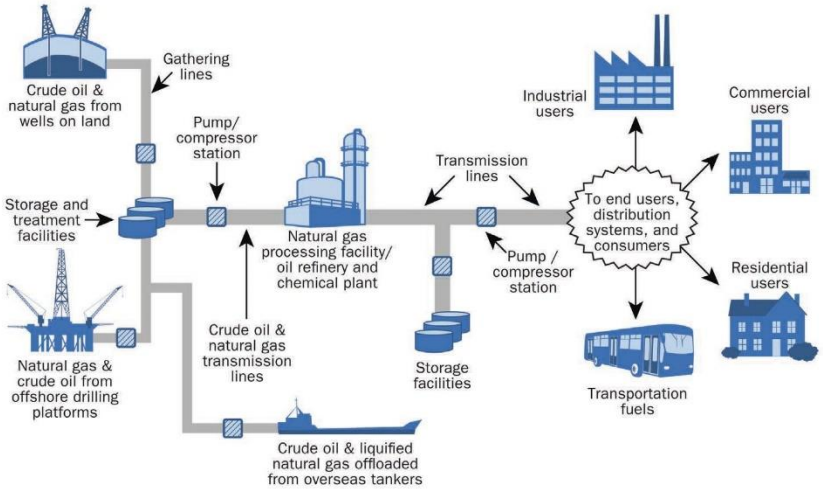
1) Modal Profile

The national pipeline system consists of more than 2.7 million miles of networked pipelines transporting hazardous liquids and toxic chemical, natural gas, and other liquids and gases for energy needs and manufacturing.

Although the majority of pipeline infrastructure is buried underground, operational elements such as compressors, metering, regulating, pumping stations, aerial crossings, and storage tanks are typically found above ground. Under operating pressure, the pipeline systems are used as a conveyance to deliver resources from source location to destination. The system is monitored and moderated through automated industrial control systems or Supervisory Control and Data Acquisition (SCADA) systems using remote sensors, signals, and preprogramed parameters to activate valves and pumps to maintain flows within tolerances.

Pipeline systems supply energy commodities and raw materials across the country to utility entities, airports, military sites, and to the Nation's industrial and manufacturing sectors (Figure 4). Vital components of the mode include pipeline systems, assets, components, and industrial automated, semi-automated, and manual control systems. Protecting vital supply chain infrastructure of pipeline operations is critical to national security and commerce.

Figure 3: The Structure of oil and gas pipeline systems movement to market.



2) Risk Profile

The national pipeline system and associated facilities are vulnerable to terrorist attacks largely due to their stationary nature, the volatility of transported products, and the dispersed nature of pipeline networks spanning urban and outlying areas. From a design–perspective, some pipeline assets are more attractive to terrorists simply due to the nature of the transported commodity and the impact of an attack on national security and commerce, and in the most extreme cases, the impact on public health. Minor pipeline system disruption may result in commodity price increases while prolonged pipeline disruptions could lead to widespread energy shortages. Short- and long-term disruptions and delays may affect other domestic critical infrastructure and industries that are dependent on pipeline system commodities.

3) Risk Scenarios

The risk scenarios inform the selection of activities to implement the risk-based priorities and address security vulnerabilities. [58]

- Vehicle Borne Improvised Explosive Device (VBIED) attack on critical infrastructure;
- Improvised Explosive Device (IED) attack on critical infrastructure;
- Cyber-attack on Supervisory Control and Data Acquisition (SCADA) systems and other operational control systems; and
- Insider threat.

B. Risk-Based Priorities

Pipeline risk-based priorities provide the programmatic focus for activities to reduce terrorism risks.

The seven risk-based priorities are:

- Security planning;
- Security training;
- Security exercises;
- Critical infrastructure protection;
- Operational detection and deterrence;
- Intelligence and security information sharing; and
- Community outreach.

[58] TSSRA 5.0 (2016).

II. Objectives, Activities, and Measuring Progress

The Pipeline Security Plan's goals and objectives reflect the risk-based priorities. Table 10 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national pipeline security.

Table 10: Pipeline Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist attacks and enhance system resilience**
Objective 1 Security Planning: **Reduce the risks from a terrorist attack on pipeline systems through security plans addressing critical infrastructure protection, operational practices (to detect and deter) and cybersecurity.**	**Activity 1:** Develop security plans, review, and update based on available information (Industry/DHS/TSA). **Outcome:** Improvement of industry security plans and security planning through incorporation of TSA Pipeline Security Guidelines into existing security plans. **Performance Measurement:** Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.[59]
Objective 2 Security Training: **Conduct training of employees to identify, prevent, absorb, respond to and recover from a terrorist attack.**	**Activity 1:** Improve the current state of the Nation's most critical pipeline systems security training program through the incorporation of TSA Pipeline Security Guidelines into existing training plans (Industry/DHS/TSA). **Outcome:** Improved capability of the industry employees to identify, prevent, absorb, respond to, and recover from a physical and/or cyber terrorist attack. **Performance Measurement:** Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.
Objective 3 Security Exercises: **Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.**	**Activity 1:** Pipeline systems participate in exercises to evaluate the preparedness for, response to, and recovery from physical and/or cyber security incidents (Industry/DHS/TSA). **Outcome:** Pipeline systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents. **Performance Measurement:** Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.

[59] https://www.tsa.gov/sites/default/files/tsapipelinesecurityguidelines-2011.pdf. Accessed July 27, 2017.

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
Objective 4 Intelligence and Information Sharing: **Maintain and enhance mechanisms for information and intelligence sharing between the pipeline industry and government.**	**Activity 1:** Provide timely and relevant information and intelligence to enhance industry's domain awareness (DHS/TSA). **Outcome:** Improved domain awareness through timely delivery of relevant intelligence and information products for pipeline industry to implement mitigation strategies to reduce risk. **Performance Measurement:** Increased timely distribution of time sensitive intelligence products.
Objective 5 Community Outreach: **Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with pipeline systems.**	**Activity 1:** Promote pipeline security awareness in communities surrounding critical pipeline assets and systems (DOE/DHS/TSA). **Outcome:** Pipeline industry, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt pipeline operations and endanger the community. **Performance Measurement:** Percentage of critical pipeline systems implementing TSA Pipeline Security Guidelines as assessed through corporate and facility security reviews.

NSTS Goal 3	Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce
Objective 1 Security Planning and Training: **Protect civil liberties and the freedom of movement of people and commerce.**	**Activity 1:** Develop policy pursuant to applicable privacy and civil liberties and civil rights laws, regulations, and policies (DHS/TSA). **Outcome:** Conformity with applicable laws. Maintaining freedom of movement of people and commerce. **Performance Measurement:** Percentage of policies cleared for compliance through TSA's OCRL.

III. Pipeline Operational Recovery Plan

Transportation services are essential to our way of life and economic prosperity. Disruptions can have debilitating effects on communities, businesses, regions, and the Nation. Operational recovery plans establish protocols for government, communities, and industry to restore transportation services as quickly as possible following a disruption.

The operational recovery from disruptions of pipeline transportation are addressed in the Pipeline Security and Incident Recovery Protocol Plan (Recovery Plan) required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*.[60] TSA and DOT's Pipeline and Hazardous Materials Safety Administration, in collaboration with pipeline operators, state, local, tribal and territorial officials, and non-profit employee organizations developed and published the Recovery Plan in March 2010.

The Nation's most critical pipelines transport raw materials and finished products for the energy and chemical industries. The effects of pipeline disruptions can ripple through the economy impacting a wide range of supply chains and critical infrastructure sectors including defense, agriculture, chemical, manufacturing, energy, and transportation. The consequences may be felt from the food markets to stock markets.

The Recovery Plan establishes a comprehensive interagency approach to minimize the consequences of disruptions of pipeline transportation, specifically focusing on actions of the Federal Government to assist the recovery operations of pipeline owners and operators. The Recovery Plan identifies ways in which the Federal Government will support the most critical interstate and intrastate natural gas and hazardous liquid (principally crude oil and refined petroleum products) transmission pipelines to restore product flows.

[60] https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf. Accessed May 4, 2017.

This Page Intentionally Left Blank

Appendix D: 2018 Intermodal Transportation Security Plan

Homeland Security

Transportation Security Administration

2018 Intermodal Transportation Security Plan

I. Introduction

A. Overview

The Intermodal Transportation Security Plan addresses the legislative requirement to provide "methods for linking the individual transportation modal security plans…and addressing the security needs of intermodal transportation."[61] This plan provides a risk-based, strategic approach to identify and protect those elements of intermodal transportation that must be protected from disruption by terrorist attacks.

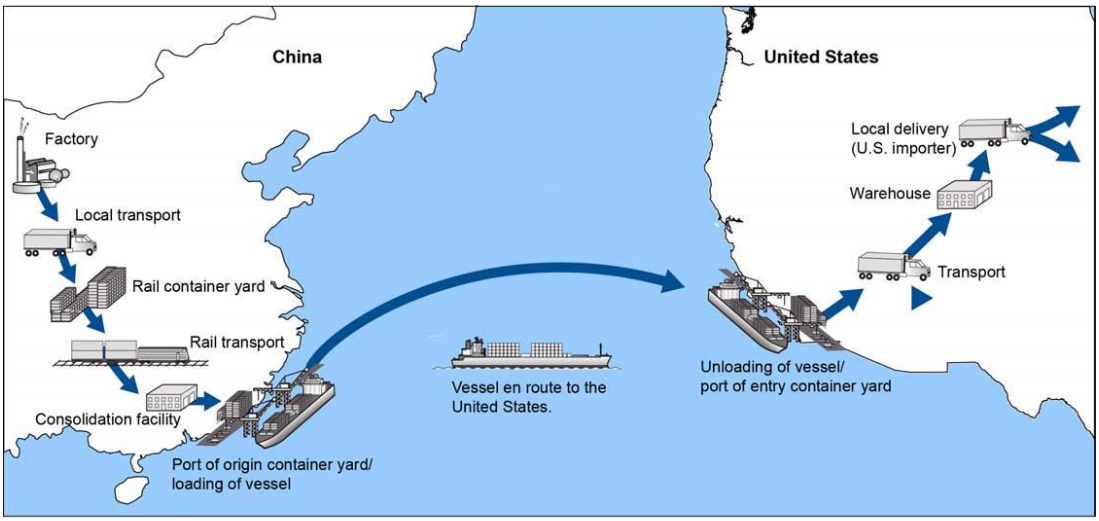
In general, intermodal transportation moves "people and goods in an energy efficient manner" and consists of "all forms of transportation [functioning] in a unified, interconnected manner."[62] Intermodal passenger operations include a mix of ground, rail, aviation, and marine transportation. When passengers move from a mass transit system to an airport, they typically leave one modal security regimen and enter another. The surface, aviation, and maritime security plans of the NSTS address the security of the infrastructure and operations providing intermodal passenger service. Due to the coverage of intermodal passenger movement in other modal security plan annexes, the Intermodal Transportation Security Plan focuses on the intermodal movement of supplies, products, mail, and parcels in supply chains.

The secure movement of raw materials and freight involves large numbers of transportation providers and associated shipping management services. These intermodal operations are an integral aspect of the global supply chains on which the United States depends for the efficient and secure movement of goods. The extensive web of supply chains that make up the global network form a complex matrix connecting suppliers of raw materials or component parts to manufacturers or processors who in turn distribute products to wholesalers, retailers, and consumers.

The Nation's public and private sectors rely on the efficiency of supply chains for the economic productivity that sustains our way of life. Efficient supply chains must be secure from, and resilient to, a variety of threats that might disrupt them. U.S. policy implemented through numerous government agencies is to strengthen the global supply chain in order to protect the welfare and interests of the American people and to secure the Nation's economic prosperity. This Intermodal Transportation Security Plan addresses the security and resilience of transportation-related elements of vital global supply chains serving the Nation.

[61] 49 U.S.C. § 114(s)(3)(H).
[62] Intermodal Surface Transportation Efficiency Act of 1991, Pub. L. No. 102-240, (Dec. 18, 1991).

Figure 4: Illustrative Example of Key Points in the Global Supply Chain



Source: GAO; Map Resources (map).

1) Global Supply Chain Profile

The global supply chain is the worldwide network of millions of individual supply chains in operation at any given time. Significant transportation elements of supply chains encompass land, sea, and air routes; shipping conveyances; transportation infrastructure; management services; and communications and information technologies.

Each transportation node or pathway in the network contributes to the time-sensitive movement of goods between initial suppliers, product developers or processors, and consumers. Increasingly sophisticated technology such as advanced intermodal containers, intelligent freight technologies, and cargo tracking technologies enable the global transportation system to move large amounts of raw materials and products rapidly and securely. This plan will focus on strategic categories of supply chains deemed to be uniquely sensitive to disruption by attacks on their transportation links.

Goods transported through supply chains are handled or managed by many entities from origin to destination such as shippers, freight forwarders, packers, and unpackers who exercise to greater or lesser extent a degree of oversight or control over the security of shipments. Global supply chain security is highly dependent on communications and information technologies to provide data on cargo manifests, handling, and movement through the various stages of transport. Global supply chains operate under a wide variety of international and domestic government rules, regulations, and protocols.

While the security practices and initiatives advanced by industry and government may be applied broadly to the Nation's domestic and international supply chains, this plan identifies certain categories of supply chains as priorities for managing transportation-related risks and evaluating the effectiveness of risk-management initiatives.

Categories of supply chains whose transportation links must be protected in the interest of national security and commerce are:

- Sensitive raw material supply chains such as certain ores, minerals, and rare Earth elements;
- Petroleum and energy product supply chains;
- Medicines, medical supplies, and human organs supply chains;
- Produce and perishable food supply chains; and
- Chemical supply chains for defense industries, public health needs, and water sanitation.

2) Risk Profile

Generally, the transportation links for supply chains are redundant, robust, and resilient. Disruptions may more often be related to labor disputes and national or international rules and protocols concerning trade practices. These threats are outside the scope of this strategy.

The terrorism-related threats directed at transportation routes or assets could disrupt commodity flows, delay supplies for vital industries or medical needs, or damage or destroy critical infrastructure. Disruption of the transportation elements of critical supply chains could impact multiple sectors. The impacts would be magnified during disasters.

The complexity of the transportation network and open access to its many nodes and pathways increase the opportunity for terrorists to exploit the supply chain for nefarious purposes. While risk mitigation measures improve defenses and resilience, by their nature, transportation elements of supply chains remain vulnerable to terrorist exploitation. Terrorists may exploit security vulnerabilities in supply chains to transport WMDs or use vehicles, trains, vessels, or planes as weapons (such as in the 9/11 attacks or the recent spate of truck ramming incidents in Europe and the United States).[63]

Intermodal maritime, land, and air operations in major transportation gateway cities (e.g., Chicago, Kansas City, Memphis, St. Louis, Indianapolis, Houston, New Orleans, and Miami) are critical pathways for many supply chains. Significant disruption in any one of these critical nodes could cause cascading consequences across transportation systems and the supply chains they serve, resulting in significant social and economic consequences. Even a small-scale attack on the transportation components of critical supply chains could significantly impact the supply of essential materials or products. Additionally, supply chain dynamics driven by shifts in supply and consumer markets, cost reduction pressures on inventories and supply sources, or labor disputes may quickly change the risk picture of the associated supply chains and their transportation components.

[63] Weapons of mass destruction: (A) any destructive device as defined in section 921 of this title; (B) any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals, or their precursors; (C) any weapon involving a biological agent, toxin, or vector (as those terms are defined in section 178 of this title); or (D) any weapon that is designed to release radiation or radioactivity at a level dangerous to human life (18 U.S.C. § 2332a).

B. Risk-Based Priorities

The transportation community secures the transportation elements of the critical supply chains through multiple layers of security programs, resources, and initiatives involving public and private sectors. To a large extent, the initiatives to assess and remediate security risks in modal infrastructure and systems address many aspects of transportation-related supply chain risks. Modal-specific strategies and activities to mitigate risks are discussed in each respective modal security plan annex to this strategy.

Transportation-related risk-management priorities for the mitigation of critical supply chain risks include:

- Security and continuity of operations planning;
- Harmonization of international supply chain security protocols;
- State of good repair of transportation infrastructure, shipping hubs, and intermodal nodes;
- Cyber and physical security;
- Cargo screening, inspection, and vetting; and
- Credentialing and access controls.

II. Programming Priorities

Global supply chain operations are driven by the dynamic, complex nature of international logistics. To meet the security challenges of international trade, the United States uses a layered security approach beginning overseas with advanced reporting (e.g., 24-Hour Advance Manifest Rule), cooperative arrangements with foreign customs organizations (e.g., the Container Security Initiative), and international protocols through U.N. organizations such as the World Customs Organization and the Uniform Postal Union.

Advanced, rules-based information technologies and policies applied in programs such as CBP's Automated Targeting System help to identify higher risk shipments and to make security-based admissibility decisions prior to the arrival of the goods in U.S. ports. Similarly, the Customs-Trade Partnership Against Terrorism (C-TPAT) is a voluntary, anti-terrorism partnership between CBP and those trade partners who agree to provide a security profile and to implement specific security measures and best practices. Through this risk segmentation method, C-TPAT members are considered to be lower-risk, and CBP is able to focus on inspection of higher-risk shipments.

Domestically, multiple layers of modal and intermodal security programs protect goods moving through supply chains. Commercial drivers who transport hazardous materials to and from secure areas of terminals or ports are vetted through programs such as the Transportation Worker Identification Credential and the Hazardous Materials Endorsement on their driver's license. These programs limit the opportunity for known terrorists to work within the industry. The maritime, freight rail, and trucking industries apply stringent security protocols to protect sensitive cargoes in transit including chemicals, fuels products, and bulk foods from access by terrorists. Government and industry security managers collaborate to protect critical transportation infrastructure to preserve the safe and efficient flow of commerce.

III. Objectives, Activities, and Measuring Progress

The Intermodal Transportation Security Plan's goals and objectives reflect the risk-based priorities. Table 11 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to intermodal transportation security.

Table 11: Global Supply Chain Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist attack and enhance system resilience**
Objective 1: **Manage risks from transportation vulnerabilities in vital supply chains.**	**Activity 1:** Identify and assess key supply chain transportation assets and systems. **Outcome:** Improve prioritizing supply chain risks. **Performance Measurement:** Estimate percent completion of identification and assessment of priority supply chains. --- **Activity 2:** Remediate physical security vulnerabilities of transportation operations to protect critical infrastructure. **Outcome:** Improve the reliability and resilience of critical supply chain nodes. **Performance Measurement:** Percent of U.S. highway bridges classified as structurally deficient (Federal Highway Administration).
Objective 2: **Encourage adoption of global supply chain transportation-related standards, regulations, guidelines, and best practices.**	**Activity 1:** Implement the International Port Security Program to assess the effectiveness of anti-terrorism measures in foreign ports, build security capacity where gaps exist, and impose conditions of entry on vessels arriving in the United States from ports with substandard security (DHS/USCG). **Outcome:** Reduce risk to foreign ports serving global supply chains. **Performance Measurement:** Security compliance rate for high-risk international maritime facilities (USCG).

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
Objective 1: **Enhance federal analysis and sharing of transportation security supply chain information to improve situational awareness of terrorist threats.**	**Activity 1:** Implement advance notice of arrival protocols including CBP's 24-Hour Advanced Manifest Rule and USCG's 96-Hour Advance Notice of Arrival to identify higher risk cargo movements for enhanced security review (CBP/USCG). **Outcome:** Use risk segmentation methods to inform scanning decisions. **Performance Measurement:** Percent of inbound cargo identified by CBP as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry (CBP).
Objective 2: **Strengthen and grow stakeholder partnerships and collaboration on supply chain resilience.**	**Activity 1:** Streamlining security processes in collaboration with public and private sector partners to enhance U.S. economic competitiveness by enabling lawful trade (DHS/CBP). **Outcome:** Reduce trade delays through security process improvements. **Performance Measurement:** Percent of imports compliant with applicable U.S. trade laws.

NSTS Goal 3	Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce
Objective 1: **Manage transportation risks in the global supply chain networks to promote the efficient flow of commerce.**	**Activity 1:** Expand risk segmentation through advanced technology to enable low-risk trade and travel (Automated Targeting System, Automated Manifest System, Air Cargo Advance Screening, and C-TPAT). **Outcome:** Improve cargo flow to the United States through risk segmentation methods. **Performance Measurement:** Percent of cargo by value imported to the United States by participants in CBP trade partnership programs. --- **Activity 2:** Streamlining security processes in collaboration with public and private sector partners to enhance U.S. economic competitiveness by enabling lawful trade (DHS/CBP). **Outcome:** Reduce trade delays through security process improvements. **Performance Measurement:** Percent of imports compliant with applicable U.S. trade laws.

Appendix E: Supplementary Information

Homeland Security

Transportation Security Administration

I. Acronyms

ATS	Aviation Transportation System
BASE	Baseline Assessment for Security Enhancement
C-TPAT	Customs-Trade Partnership Against Terrorism
CBP	U.S. Customs and Border Protection
CBRN	Chemical, Biological, Radiological, and Nuclear
CFR	Code of Federal Regulations
COP	Common Operating Procedure
CWMD	Countering Weapons of Mass Destruction Office
DHS	Department of Homeland Security
DHS TRIP	Department of Homeland Security Travelers Redress Inquiry Program
DNDO	Domestic Nuclear Detection Office
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HMC	Highway and Motor Carrier
HTUA	High Threat Urban Areas
HVE	Homegrown Violent Extremist
ICS	Industrial Control Systems
IED	Improvised Explosive Device
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
MIRP	Maritime Infrastructure Recovery Plan
MSRAM	Maritime Security Risk Analysis Model
MSRO	Maritime and Security Response Operations
MTPR	Mass Transit and Passenger Rail
MTS	Maritime Transportation System
NDRF	National Disaster Recovery Framework
NIPP	National Infrastructure Protection Plan
NPS	National Preparedness System
NRF	National Recovery Framework
NSAS	National Strategy for Aviation Security
NSPTS	National Strategy for Public Transportation Security
NSRTS	National Strategy for Railroad Transportation Security
NTAT	Non-Traditional Aviation Technology
NTRS	National Transportation Recovery Strategy
OTRB	Over-the-Road Bus
R&D	Research and Development
RSSM	Rail Security-Sensitive Material
SCADA	Supervisory Control and Data Acquisition
SLTT	State, local, tribal, and territorial
TSA	Transportation Security Administration
TSSRA	Transportation Sector Security Risk Assessment
UAS	Unmanned Aircraft Systems
USCG	U.S. Coast Guard
Rap Back	Record of Arrest and Prosecution

VBIED	Vehicle Borne Improvised Explosive Device
WMD	Weapon of Mass Destruction

II. Roles and Responsibilities

A. Federal Government

DHS provides strategic security planning and guidance, promotes a national unity of effort, and coordinates the overall federal effort to promote the security and resilience of the Nation's transportation assets, infrastructure, and systems. Many other federal departments contribute to transportation security, including DOT, the Department of State, the Department of Justice, the Department of Energy, the Department of Defense, the Department of Commerce, and the Department of Agriculture. In carrying out these responsibilities, the Federal Government:

- Evaluates national capabilities, opportunities, and challenges in securing and making resilient nationally significant transportation infrastructure;
- Provides guidance for and analyzes the threats, vulnerabilities, and consequences to critical infrastructure from terrorism and other threats;
- Identifies transportation security and resilience functions that are necessary for effective national recovery;
- Participates in national and international organizations that plan, implement, and monitor security policies;
- Collects, analyzes, and shares security intelligence and information; and
- Provides grant funding to support risk management activities.

B. SLTT Governments

SLTT government entities are the first to respond to terrorist incidents. Consequently, SLTT governments are best positioned to address specific homeland security needs and to assume the lead for local preparedness. SLTT authorities assist in the identification of critical transportation assets, determination of security gaps and priorities, and development of security, response, and recovery plans to protect those assets. Specific responsibilities of SLTT governments are further discussed in the National Infrastructure Protection Plan 2013, Partnering for Critical Infrastructure Security and Resilience.

C. Industry

Transportation owners and operators, both public and private, have principal responsibility for the safety and security of the people using their services. The specific roles and responsibilities vary based on the nature of the service provided and the associated security risks. Industry associations represent many owners and operators in collaborative forums with federal or SLTT government entities. Since the 9/11 attacks, owners and operators have undertaken significant steps, many voluntary, to reduce security risks. Those steps include, for example:

- Conducting risk assessments;
- Developing security plans, employee training, and exercise programs;

- Establishing continuity plans and programs that sustain critical transportation functions during a security-related incident; and
- Participating in coordination bodies and mechanisms such as Sector Coordinating Councils, Aviation Security Advisory Committee, Peer Advisory Groups, and Area Maritime Security Councils.

III. Glossary of Terms

Many of the definitions in this Glossary are from federal laws, executive or departmental directives, or the DHS Lexicon.

Asset. Person, structure, facility, information material, or process that has value. (Source: DHS Lexicon, 2017)

Baseline Risk. Current level of risk that takes into account existing risk mitigation measures. (Source: DHS Lexicon, 2017)

Consequence. Effect if an event, incident, or occurrence. (Source: DHS Lexicon, 2017)

Control Systems. Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include SCADA systems, Process Control Systems, and Distributed Control Systems. (Source: 2009 NIPP)

Critical Infrastructure. Systems and assets, whether physical or virtual, so vital to the United States, 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. (Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e))

Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)

Cyber System. Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services. Examples include business systems, control systems, collision avoidance systems, SCADA systems, fire suppression systems, industrial control systems, signals and access control systems. (Source: 2009 NIPP)

Executive Order 13636. Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing, develop a technology-neutral cybersecurity framework, and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013)

Federal Departments and Agencies. Any component of the United States Government that is an "agency" under 44 U.S.C. §3502(1) other than those considered to be independent regulatory agencies as defined in 44 U.S.C. §3502(5). (Source: PPD-21, 2013)

Fusion Center. Physical or logical facility, encompassing all necessary infrastructure required to facilitate nationwide information-sharing between one or more federal, state, and/or local law enforcement entities, dedicated to the integration of multiple diverse data sources within a defined functional domain. (Source: DHS Lexicon, 2017)

Hazard. Natural or manmade source or cause of harm or difficulty. (Source: DHS Lexicon, 2017)

Incident. A natural, technological, or human-caused occurrence that may cause harm and that may require action. (Source: DHS Lexicon, 2017)

Infrastructure. The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States, the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2017)

Mitigation. Capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (Source: PPD-8, 2011)

Network. A group of components that share information or interact with each other to perform a function. (Source: 2009 NIPP)

Partnership. Close cooperation between parties having common interests in achieving a shared vision. (Source: NIPP 2013)

Performance Measurement. The on-going monitoring and reporting of program accomplishment, particularly progress toward pre-established goals. (Source: Performance Measurement and Evaluation. Definitions and Relationships, GA-11-646SSP)

Presidential Policy Directive 8 (PPD-8). Facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation, including acts of terrorism, cyber-attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)

Presidential Policy Directive 21 (PPD-21). Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with critical infrastructure owners and operators and SLTT entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 2013)

Prevention. Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (Source: PPD-8, 2011)

Protection. Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (Source: PPD-8, 2011)

Recovery. Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to: rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (Source: PPD-8, 2011)

Regional. Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key stakeholders within the given location. (Source: Regional Partnerships: Enabling Regional Critical Infrastructure Resilience, RC3, March 2011)

Resilience. The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Source: PPD-21, 2013)

Response. Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (Source: PPD-8, 2011)

Risk. Potential for an unwanted outcome as determined by its likelihood and the consequences. (Source: DHS Lexicon, 2017)

Risk Mitigation. Application of measure or measures to reduce the likelihood of an unwanted occurrence and/or its consequences (Source: DHS Lexicon, 2017)

Sector. A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the National Plan addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: Adapted from the 2009 NIPP)

System. Aggregation of end products enabling products to achieve a given purpose. (Source: DHS Lexicon, 2017)

Terrorism. Premeditated threat or act of violence, against persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (Source: DHS Lexicon, 2017)

Threat. Indication of potential harm life, information, operations, the environment, and/or property. (Source: DHS Lexicon, 2017)

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (Source: DHS Lexicon, 2017)

Annex I: 2018 National Strategy for Public Transportation Security

Homeland Security

Transportation Security Administration

Executive Summary

The National Strategy for Public Transportation Security (NSPTS) provides strategic-level public transportation security-planning guidance, as required by 6 U.S.C. § 1133. The NSPTS aids government stakeholders in managing risks to public transportation systems and in maximizing the ability of public transportation system owners and operators to mitigate damage resulting from a terrorist attack or other major incident.

Through four principal activities—analyzing threats, assessing vulnerabilities, information sharing, and determining risk-based priorities—the NSPTS achieves the strategic objectives of the legislative guidance. The Mass Transit and Passenger Rail Security Plan, Appendix C of the National Strategy for Transportation Security (NSTS), provides prioritized goals, objectives, and activities to operationalize the NSPTS. Section VI of the NSPTS, Implementation, provides the strategic guidance for reducing security risks in the four principal security activities.

World events illustrate that terrorists continue to present a persistent and evolving threat to public transportation security by demonstrating their ability to adapt and innovate to overcome security practices. Despite improvements in public transportation security through the use of core security principles and threat-specific security practices, the dynamic nature of the threat environment continues to pose a significant challenge. Growing and diverse ridership demands, improvements in public transportation safety, and the modernization of aging systems will compete with security efforts for limited public resources.

The security goals of the Mass Transit Passenger Rail Security Plan in the 2018 NSTS are predicated on the vigilance of security partners to: monitor and update security policies, processes, and activities; be forward-thinking about the evolving security environment; and consider the security capabilities and resource limitations of industry partners.

2018 National Strategy for Public Transportation Security

Table of Contents

I. Legislative Requirements

The NSPTS addresses the requirement for a "National Strategy" established by the 9/11 Act, as codified at 6 U.S.C. § 1133, and provides the strategic framework necessary for development of the passenger transportation aspects of the Mass Transit and Passenger Rail Security Plan required by the IRTPA.[1]

> (a) National Strategy. Not later than 9 months after August 3, 2007, and based upon the previous and ongoing security assessments conducted by the Department and the Department of Transportation, the Secretary, consistent with and as required by section 114(t) [*sic*] of Title 49, United States Code, shall develop and implement the modal plan for public transportation, entitled the "National Strategy for Public Transportation Security."
> (b) Purpose.
> (1) Guidelines. In developing the National Strategy for Public Transportation Security, the Secretary shall establish guidelines for public transportation security that—
> (A) minimize security threats to public transportation systems; and
> (B) maximize the abilities of public transportation systems to mitigate damage resulting from terrorist attack or other major incident.
> (2) Assessments and consultations. —In developing the National Strategy for Public Transportation Security, the Secretary shall—
> (A) use established and ongoing public transportation security assessments as the basis of the National Strategy for Public Transportation Security; and
> (B) consult with all relevant stakeholders, including public transportation agencies, nonprofit labor organizations representing public transportation employees, emergency responders, public safety officials, and other relevant parties.
> (c) Contents. In the National Strategy for Public Transportation Security, the Secretary shall describe prioritized goals, objectives, policies, actions, and schedules to improve the security of public transportation.
> (d) Responsibilities. The Secretary shall include in the National Strategy for Public Transportation Security a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, tribal governments, and appropriate stakeholders. The plan shall also include—
> (1) the identification of, and a plan to address, gaps and unnecessary overlaps in the roles, responsibilities, and authorities of Federal agencies; and
> (2) a process for coordinating existing or future security strategies and plans for public transportation, including the National Infrastructure Protection Plan required by Homeland Security Presidential Directive-7; Executive Order No. 13416: Strengthening Surface Transportation Security dated December 5, 2006; the Memorandum of Understanding between the Department and the Department of

[1] 49 U.S.C. 114(s). As previously noted, the IRTPA required preparation and implementation of transportation modal security plans to address security risks including threats, vulnerabilities, and consequences.

Transportation on Roles and Responsibilities dated September 28, 2004; and subsequent annexes and agreements.

(e) Adequacy of existing plans and strategies. In developing the National Strategy for Public Transportation Security, the Secretary shall use relevant existing risk assessments and strategies developed by the Department or other Federal agencies, including those developed or implemented pursuant to section 114(t) [*sic*] of Title 49, United States Code, or Homeland Security Presidential Directive-7.

(f) Funding. —There is authorized to be appropriated to the Secretary to carry out this section $2,000,000 for fiscal year 2008.

II. Introduction

The NSPTS provides a strategic-level framework to manage risks to public transportation systems from terrorist threats and to maximize the ability of owners and operators to mitigate damage resulting from a terrorist attack or other major incident. The Mass Transit and Passenger Rail Security Plan (Appendix C of the NSTS) implements the public transportation security priorities of the NSPTS. The legislative definition of "railroad transportation" includes passenger and commuter rail services operating on the "general railroad system of transportation."[2] Therefore, passenger rail security is addressed in the National Strategy for Railroad Transportation Security, Annex II to the NSTS.

For purposes of the NSPTS, the terms public transportation, public transit, and mass transit are used interchangeably.[3]

Public transportation refers to:

- Heavy rail (subways and metros);
- Light rail (trolleys and streetcars);
- Monorail;
- Cable cars;
- Inclined planes (funiculars);
- Automated guideway systems;
- Intercity buses; and
- Demand response services.

[2] 49 U.S.C. § 20102.
[3] 49 U.S.C. § 5302.

III. Public Transportation Overview

Public transportation in America is critically important to our way of life, as evidenced by the number of riders on the Nation's public transportation systems. A successful terrorist attack would have a profound impact on public transportation ridership and a negative economic impact nation-wide. Securing public transportation systems from terrorist attacks is vitally important and a task that demands constant vigilance, innovation, and dedication.

A. Statistics

According to the American Public Transportation Association (APTA), 2016 Public Transportation Fact Book, people boarded public transportation 35 million times each workday. In 2016, Americans took 10.4 billion trips on public transportation. In 2014, the five largest transit agencies—Metropolitan Transportation Authority New York City Transit, Chicago Transit Authority, Los Angeles County Metropolitan Transportation Authority, Washington Metropolitan Area Transit Authority, and the Massachusetts Bay Transportation Authority—totaled over 5.4 billion unlinked passenger trips.[4]

B. Risk Profile

Public transportation systems are inherently difficult to secure because of their open architecture design which allows defined patterns of movement. Many public transportation systems have multiple access points, which are essential to efficient operations. Underground stations, underwater tunnels, and transit bridges also present a unique security challenge. Public transportation stations and bus stops may be located in close proximity to other targets of interest, such as other transportation hubs, critical infrastructure, and symbolic targets.

Primary risk scenarios for public transportation include sabotage, armed assaults, cyber-attacks, chemical/biological attacks, or attacks using improvised explosive or incendiary device(s) which are primarily intended to cause fatalities and injure riders.

Effective and measurable risk-based priorities are described in Section VI, Implementation. The risk-based priorities serve as a framework for government and industry stakeholders to develop plans, policies, and procedures to reduce security risks.

[4] 2016 Public Transportation Fact Book, 67th Edition, February 2017. http://www.apta.com/resources/statistics/Documents/FactBook/2016-APTA-Fact-Book.pdf. Accessed May 23, 2017. Information in the Fact Book is based on data from the FTA's National Transit Database for 2014.

IV. Roles and Responsibilities

A. Federal Government

The Federal Government is responsible for strategic planning and coordinating the efforts of government entities, industry, and communities to secure the transportation systems and to improve the resilience of transportation networks. Strategic security planning and guidance promotes a national unity of effort and enhances the federal effort to secure the Nation's transportation assets, infrastructure, and systems. Other federal departments contributing to public transportation security efforts include the Federal Transit Administration, Federal Railroad Administration, Federal Emergency Management Agency, and the Federal Bureau of Investigation.

Federal Government responsibilities include:

- Assessing intelligence to identify individuals who pose a threat to transportation security;
- Sharing threat information and communicating threat countermeasures to stakeholders;
- Developing and enforcing security-related regulations and requirements;
- Promoting security best practices;
- Identifying and addressing security gaps and unnecessary overlaps in federal roles and responsibilities; and
- Providing grant funding to support risk management activities.

B. State, Local, Tribal, and Territorial Government Entities

State, Local, Tribal, and Territorial (SLTT) government entities are the first to respond to terrorist incidents. Consequently, SLTT governments are best positioned to identify and address specific public transportation security needs and to lead local preparedness efforts.

SLTT responsibilities include:

- Determining security gaps and identifying transportation security priorities;
- Developing security, response, and recovery plans to protect public transportation assets; and
- Collaborating with Federal Government and industry to promote public transportation security.

C. Industry

Public transportation owners and operators have the primary responsibility for the safety and security of people using their services. Roles and responsibilities vary based on the nature of the services provided, relationships with local law enforcement, and the nature of the security risks. Industry associations represent many owners and operators in collaborative forums with federal and SLTT Government entities.

Regulations require transportation system operators to take specific actions to provide for passenger safety and security. Operators take significant voluntary steps to reduce security risks and increase system resilience.

Industry responsibilities include:

- Conducting risk assessments;
- Developing security plans, training and exercise programs;
- Establishing continuity plans and programs that sustain critical transportation functions during a security-related incident;
- Participating in coordination bodies and mechanisms such as the Transit Policing and Security Peer Advisory Group (PAG);
- Acting on, and sharing, intelligence reports, security awareness messages, and other federal and SLTT transportation security communication; and
- Incorporating "best practices" into day-to-day operations.

V. Implementation

The NSPTS encourages frequent sharing of intelligence and information with public transportation owners and operators, continuous analysis and communication of threats to all transportation stakeholders, establishing common risk-based priorities to ensure appropriate resourcing and administration of security measures, and assessment of risks to public transportation systems through on-site security assessments and reviews. Figure 1 illustrates the high-level security activities that are necessary to operationalize the NSPTS and are detailed further in the Mass Transit and Passenger Rail Security Plan.

The Mass Transit and Passenger Rail Security Plan operationalizes the NSPTS through prioritized goals with objectives and supporting activities, which are monitored to ensure relevancy to risks and consistency in performance. Figure 1 provides an illustration of the four principal mass transit and passenger rail activities necessary to operationalize this strategy.

Figure 1: Four Principal Activities Operationalizing the National Strategy for Public Transportation Security

A. Information Sharing

Evolving and unpredictable security threats posed to public transportation and the expanding environment of public transportation operating systems call for continuous sharing of security information and intelligence between government and public transportation stakeholders. The

NSTS identifies the need for collaboration of transportation security partners to achieve a common understanding of challenges, impacts, and feasible solutions.

To achieve these goals, as required by the 9/11 Act, the Transportation Security Administration (TSA) developed the Transportation Security Information Sharing Environment report to "promote sharing of transportation security information between the Department of Homeland Security (DHS) and public and private stakeholders."[5] The report describes the process and products available for sharing with stakeholders pertinent threat and incident information, recommended practices, protective measures, and domain awareness updates.

Information is exchanged domestically and internationally through a variety of venues hosted by government and industry:

- The Mass Transit and Passenger Rail Government Coordinating Council (GCC) and Sector Coordinating Council meetings are held as needed in joint sessions to discuss priorities and efforts to improve security and reduce risk.
- RAILPOL, a European based network of railway police forces, comprises members from the European Union Member States, Switzerland, and the United States. Strategic leadership conferences are held annually to exchange operational ideas and share best practices in countering terrorism in the railway network.
- The Surface Transportation/Public Transportation (ST-PT) Information Sharing and Analysis Center (ISAC) is a trusted entity that provides to its constituency a 24/7 Security Operating Capability to receive and disseminate critical information/intelligence for incidents, threats, and vulnerabilities.
- The Transit Rail and Intelligence Awareness Daily reports are a product of the ST-PT ISAC, which provide stakeholders with a quick, easy-to-read synopsis in three fundamental areas—suspicious activities, terrorism and counterterrorism analysis, and general security awareness information. This daily report is developed through analysis of numerous intelligence resources.
- The Transit Policing and Security Peer Advisory Group (PAG) brings together the expertise of transit police chiefs and security directors from mass transit and passenger rail systems from the United States, Canada, and the United Kingdom and acts as an effective communication instrument for liaison with TSA and other Federal Government agencies.
- Security Awareness Messages, providing security information about the need for heightened awareness, are developed by TSA and delivered to industry partners. These messages encourage continued vigilance and timely reporting of suspicious incidents, reemphasize existing security measures, and/or recommend voluntary protective measures over designated time periods of heightened alert such as Memorial Day and Independence Day.

[5] 49 U.S.C § 114(u).

B. Threat Analysis

The Federal Government issues incident-specific and recurring assessments of the domestic and international threats to mass transit and passenger rail systems throughout the year. These assessments help federal, state, and local government security officials and industry professionals protect U.S. railroad systems from attacks. These products describe key terrorist actors and group ideologies, recent attacks, modes of attack, and other tactics, techniques, and procedures used by terrorists and provide a threat level based on these analyses.

C. Security Assessments

Risk assessments consider various threat scenarios and the vulnerabilities and consequences attributed to them. TSA's primary risk assessment tool is the Transportation Sector Security Risk Assessment. The process used to perform the assessment elicits detailed analyses of the vulnerabilities to and consequences of an attack (threat) on a transportation target. The results of the assessments are used to compare risks across the modes, establish risk-based priorities, and, decide on mode-specific risk mitigation actions. Other threat and risk assessments, such as DHS's National Risk Estimates, the Strategic National Risk Assessment, and modal threat assessments provide additional sources for security planning and programming decisions. These products are augmented by intelligence-driven, time-sensitive analyses of emerging events.

The Federal Government's primary method of assessing vulnerabilities of public transportation systems in the operating environment is TSA's Baseline Assessment for Security Enhancement (BASE) program. The program is designed to establish a security standard for individual system security programs and assess progress. This voluntary comprehensive review of security programs focuses on multiple categories identified by the surface modal transportation communities as fundamental for a sound security program.

Using a set of industry best practices as a benchmark, TSA conducts these periodic voluntary BASE assessments of public transportation locations and operations that include reviews of security plans and their implementation. Stakeholders are provided with a detailed report and recommended improvements specific to their operations enhancing their ability to establish mitigation priorities.

D. Risk-Based Priorities

Seven risk-based priorities provide the foundation for supporting objectives and activities in the Mass Transit and Passenger Rail Security Plan within the NSTS. Although the means to achieve the desired end results may vary among the different modes, the overarching vision is for TSA and its stakeholders to work together to implement programs, procedures, and processes for addressing these priorities.

The seven risk-based priorities are:

- Security planning;

- Security training;
- Security exercises;
- Critical infrastructure protection;
- Operational deterrence;
- Intelligence and security information sharing; and
- Community outreach.

E. Other Actions

Transit Security Grant Program

The Transit Security Grant Program, authorized by section 1406 of the 9/11 Act and administered by the Federal Emergency Management Agency in collaboration with TSA, directly supports public transportation operational and capital infrastructure security activities. Program funds are appropriated annually and awarded to eligible public transit agencies (which include intracity bus, commuter bus, ferries, and all forms of passenger rail) to support the creation of sustainable, risk-based efforts to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase the resilience of transit infrastructure.

Security Regulations

Part 1580 of Title 49 of the Code of Federal Regulations establishes rules for the security of passenger rail transportation. In pertinent part, the rules apply to passenger railroad carriers and to each operator of a rail transit system including; heavy rail transit, light rail transit, automated guideway, cable car, inclined plane, funicular, and monorail systems. The rule, in pertinent part, covers appointment of security coordinators, and security-related reporting requirements.

The 9/11 Act directs the Secretary of Homeland Security to issue regulations for a public transportation security training program to prepare public transportation employees, including frontline employees, to appropriately observe, assess, and report suspicious persons, activities, and events. Additionally, the 9/11 Act requires public transportation agencies, determined by the Secretary of Homeland Security to be at high risk for terrorism, to conduct vulnerability assessments and develop comprehensive security plans. TSA is developing regulations to implement these mandates.

VI. Research and Development

Transportation security and resilience is enhanced through the identification and application of existing, emerging technologies, and processes that address capability gaps. Technology enhancements lead to operational efficiencies and often reduce costs. Both government and the transportation industry participate in Research and Development (R&D) working groups to identify gaps in transportation security and resilience capabilities. For example, the joint Surface Transportation Systems R&D Working Group, which includes representation from DHS, DOT, and public and private partners, is the primary means of identifying security capability gaps in the surface modes of transportation. The finalized capability gaps serve as a basis for developing R&D project requirements for consideration by the funding organization (e.g., DHS S&T, TSA, and DOT).

VII. Performance

The Mass Transit Passenger Rail Security Plan provides outcome-based activities and measurement approaches to indicate progress in achieving National Strategy for Public Transportation Security goals. These measures continue to be refined and developed. In some cases, data streams will need to be established to reflect progress towards outcomes. Because many initiatives are voluntary, industry involvement and investment is needed in refining outcomes, developing methodologies, and collecting data.

VIII. Acronyms

APTA	American Public Transportation Association
BASE	Baseline Assessment for Security Enhancement
DOT	Department of Transportation
GCC	Government Coordinating Council
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAC	Information Sharing and Analysis Center
NSPTS	National Strategy for Public Transportation Security
NSTS	National Strategy for Transportation Security
PAG	Transit Policing and Security Peer Advisory Group
R&D	Research and Development
SLTT	State, local, tribal, and territorial
ST-PT	Surface Transportation/Public Transportation
TSA	Transportation Security Administration

Annex II: 2018 National Strategy for Railroad Transportation Security

Homeland Security

Transportation Security Administration

Executive Summary

The National Strategy for Railroad Transportation Security (NSRTS) provides strategic-level railroad security planning guidance as required by 6 U.S.C. § 1161. Through four principal activities— information sharing, analyzing threats, assessing vulnerabilities, and determining risk-based priorities—the NSRTS achieves the strategic requirements and objectives identified in the statute. The NSRTS is operationalized by the Freight Rail Security Plan and the Mass Transit and Passenger Rail Security Plan for the freight and passenger components, respectively, of railroad transportation. These plans are contained in the Surface Security Plan, Appendix C of the National Strategy for Transportation Security (NSTS). They provide prioritized security goals and activities. Section V of the NSRTS discusses these relationships and implementation strategies in greater detail.

Terrorists and hackers internationally have demonstrated interest in railroad transportation as a potential target. There is a continued need to address evolving threats to freight, passenger, and commuter railroad operations. The inherently open nature of railroad infrastructure presents a security challenge to both industry and government. The miles of track and supporting infrastructure in the rail network necessitates a prudent application of limited security resources to protect the system's components at greatest risk. The principal purpose of this strategy is to foster cooperative efforts between government departments and agencies and freight and passenger railroads and rail industry organizations on mitigating risks associated with the threat of terrorism and serious cyber-attacks.

The security goals common to the railroad security plans in the 2018 NSTS call upon us to: monitor and update policies, processes, and activities when necessary; be forward thinking in our reexamination and application of those policies, processes and activities; and consider the security capabilities and resource limitations of industry partners.

2018 National Strategy for Railroad Transportation Security

Table of Contents

I. Legislative Requirements

The NSRTS addresses the "National Strategy" requirements established by the 9/11 Act, as codified at 6 U.S.C. § 1161 and provides the strategic framework necessary for development of the Freight Rail and Mass Transit Passenger Rail Security Plans as required by 49 U.S.C. § 114(s).[1]

(b) National Strategy.
(1) Requirement. Not later than 9 months after the date of enactment of this Act and based upon the assessment conducted under subsection (a), the Secretary, consistent with and as required by section 114(t)[*sic*] of title 49, United States Code, shall develop and implement the modal plan for railroad transportation, entitled the "National Strategy for Railroad Transportation Security."
(2) Contents. The modal plan shall include prioritized goals, actions, objectives, policies, mechanisms, and schedules for, at a minimum—
(A) improving the security of railroad tunnels, railroad bridges, railroad switching and car storage areas, other railroad infrastructure and facilities, information systems, and other areas identified by the Secretary as posing significant railroad-related risks to public safety and the movement of interstate commerce, taking into account the impact that any proposed security measure might have on the provision of railroad service or on operations served or otherwise affected by railroad service;
(B) deploying equipment and personnel to detect security threats, including those posed by explosives and hazardous chemical, biological, and radioactive substances, and any appropriate countermeasures;
(C) consistent with section 1517, training railroad employees in terrorism prevention, preparedness, passenger evacuation, and response activities;
(D) conducting public outreach campaigns for railroads regarding security, including educational initiatives designed to inform the public on how to prevent, prepare for, respond to, and recover from a terrorist attack on railroad transportation;
(E) providing additional railroad security support for railroads at high or severe threat levels of alert;
(F) ensuring, in coordination with freight and intercity and commuter passenger railroads, the continued movement of freight and passengers in the event of an attack affecting the railroad system, including the possibility of rerouting traffic due to the loss of critical infrastructure, such as a bridge, tunnel, yard, or station;
(G) coordinating existing and planned railroad security initiatives undertaken by the public and private sectors;
(H) assessing—
(i) the usefulness of covert testing of railroad security systems;
(ii) the ability to integrate security into infrastructure design; and

[1] 49 U.S.C. §114(s). As previously noted, the IRTPA amended section 114 to require preparation and implementation of transportation modal security plans to address security risks, including threats, vulnerabilities, and consequences.

(iii) the implementation of random searches of passengers and baggage; and

(I) identifying the immediate and long-term costs of measures that may be required to address those risks and public and private sector sources to fund such measures.

(3) Responsibilities. Secretary shall include in the modal plan a description of the roles, responsibilities, and authorities of Federal, State, and local agencies, government sponsored entities, tribal governments, and appropriate stakeholders described in subsection (c). The plan shall also include—

(A) the identification of, and a plan to address, gaps, and unnecessary overlaps in the roles, responsibilities, and authorities described in this paragraph;

(B) a methodology for how the Department will work with the entities described in subsection (c), and make use of existing Federal expertise within the Department, the Department of Transportation, and other appropriate agencies;

(C) a process for facilitating security clearances for the purpose of intelligence and information sharing with the entities described in subsection (c), as appropriate;

(D) a strategy and timeline, coordinated with the research and development program established under section 1518, for the Department, the Department of Transportation, other appropriate Federal agencies and private entities to research and develop new technologies for securing railroad systems; and

(E) a process for coordinating existing or future security strategies and plans for railroad transportation, including the National Infrastructure Protection Plan required by Homeland Security Presidential Directive–7; Executive Order No. 13416: ''Strengthening Surface Transportation Security'' dated December 5, 2006; the Memorandum of Understanding between the Department and the Department of Transportation on Roles and Responsibilities dated September 28, 2004, and any and all subsequent annexes to this Memorandum of Understanding, and any other relevant agreements between the two Departments.

(c) Consultation with stakeholders. In developing the National Strategy required under this section, the Secretary shall consult with railroad management, nonprofit employee organizations representing railroad employees, owners or lessors of railroad cars used to transport hazardous materials, emergency responders, officials of security-sensitive materials, public safety officials, and other relevant parties.

(d) Adequacy of Existing Plans and Strategies. In developing the risk assessment and National Strategy required under this section, the Secretary shall utilize relevant existing plans, strategies, and risk assessments developed by the Department or other Federal agencies, including those developed or implemented pursuant to section 114(t) [*sic*] of title 49, United States Code, or Homeland Security Presidential Directive–7, and, as appropriate, assessments developed by other public and private stakeholders.

(e) Report.

(1) Contents. Not later than 1 year after the date of enactment of this Act, the Secretary shall transmit to the appropriate congressional committees a report containing—

(A) the assessment and the National Strategy required by this section; and

(B) an estimate of the cost to implement the National Strategy.

(2) Format. The Secretary may submit the report in both classified and redacted formats if the Secretary determines that such action is appropriate or necessary.

(f) Annual Updates. Consistent with the requirements of section 114(t) [*sic*] of title 49, United States Code, the Secretary shall update the assessment and National Strategy each

year and transmit a report, which may be submitted in both classified and redacted formats, to the appropriate congressional committees containing the updated assessment and recommendations.

(g) Funding. Out of funds appropriated pursuant to section 114(w) of title 49, United States Code, as amended by section 1503 of this title, there shall be made available to the Secretary to carry out this section $5,000,000 for fiscal year 2008.

II. Introduction

The NSRTS provides a strategic-level framework to prevent terrorist acts on freight and passenger railroad systems and to enhance the abilities of railroads to mitigate damage. The NSRTS provides guidance for development of the supporting Freight Rail and Mass Transit and Passenger Rail Security Plans located in Appendix C of the NSTS through prioritized goals, supporting activities, and other requirements as set forth in legislation.[2]

As used in this document, the term railroad includes any form of non-highway ground transportation that runs on rails or electromagnetic guideways, including freight rail, passenger and commuter rail, or other short-haul railroad passenger service in a metropolitan or suburban area. It does not include transit operations in urban areas that are not connected to the general railroad system of transportation (e.g., streetcars, subways, metros, and monorails).[3]

[2] 6 U.S.C. § 1161 and 6 U.S.C. § 1133. Transit operations are addressed in the National Strategy for Public Transportation Security.
[3] 49 U.S.C. § 20102.

III. Railroad Transportation Overview

The Nation's railroad security program is built on strong partnerships with private and public stakeholders to identify and manage risk in this critical transportation mode. Government partners work with the Nation's railroad carriers to identify and reduce physical and cyber-related vulnerabilities and to advance capabilities to prevent and mitigate the risk of a possible attack. Security and emergency preparedness plans, information sharing, assessments, training, exercises, and community engagement are examples of activities in which railroads and government agencies work to improve security posture and narrow risk profile – for the prevention of attacks and mitigation of potential consequences.

A. Statistics

The freight railroad network is a complex system that includes both physical and cyber infrastructure. There are 574 freight railroads that operate in the United States. The seven "Class I" railroads—BNSF Railway, Canadian National Railway, Canadian Pacific Railway, CSX Transportation, Kansas City Southern Railway, Norfolk Southern Railway, and Union Pacific Railroad—account for 69 percent of freight rail mileage, 90 percent of employees, and 94 percent of revenue.[4] Class I railroads operate in many states over thousands of track miles. Regional railroads (21) and local railroads (546) range in size from operations handling a few carloads to multi-state operators. The railroads form an integrated system of nearly 138,000 miles of track over which 28 million carloads, including 2.5 million containing hazardous materials travel each year.[5] In 2016, railroads transported approximately 75,000 carloads containing Rail Security-Sensitive Materials (RSSM) which are regulated under 49 CFR Part 1580.[6] In proportion to the overall shipment volumes each year, RSSM shipments constitute 3% of all hazardous material shipments and less than 3/10 of a percent of all shipments.

Passenger rail is divided into two categories: inter-city rail (Amtrak and Alaska Railroad) and commuter rail service. Inter-city provides long-distance service, while commuter railroads provide service over shorter distances, usually less than 100 miles. Freight railroads provide the tracks for most passenger rail operations; however, passenger rail agencies are not wholly dependent on freight rail infrastructure and corridors for operational feasibility and sometimes control, operate, and maintain track, facilities, construction sites, utilities, and computerized networks essential to their own operations.

The sole medium- and long-distance intercity passenger railroad in the contiguous United States is Amtrak, which has an annual ridership of approximately 31.3 million.[7] Amtrak operates a nationwide rail network, serving more than 500 destinations in 46 states, the District of

---

[4] https://www.aar.org/todays-railroads/our-network?t=typesofrailroads. Accessed December 3, 2015.
[5] https://www.aar.org/BackgroundPapers/Railroads%20Moving%20America%20Safely.pdf. Accessed May 4, 2017.
[6] Transportation Security Administration, RAILS information database, 2016.
[7] https://www.amtrak.com/ccurl/1006/987/National-Fact-Sheet-FY2016.pdf. Accessed May 4, 2017.

Columbia, and three Canadian provinces on more than 21,300 track-miles.[8] Freight railroads own and control 72 percent of the track on which Amtrak operates.[9] A notable exception is the North East Corridor, an electrified railway line in the Northeast megalopolis of the United States. Owned primarily by Amtrak, the Northeast Corridor is an electrified railway line and runs from Boston through New York City, Philadelphia, Baltimore, and terminates in Washington, D.C. On a daily basis it is host to 800,000 riders in over 2,000 passenger trains including commuter rail services operated by the Massachusetts Bay Transportation Authority, Shore Line East, Metro North Railroad, New Jersey Transit, Southeastern Pennsylvania Transportation Authority, and Maryland Area Regional Commuter Train.[10]

Rail passenger transportation services are provided by 28 commuter railroads operating in several metropolitan areas bearing a cumulative annual ridership of nearly 4.7 billion.[11] Many of the commuter railroads operate or plan to operate at least partially on freight-owned corridors. Additionally, most of the higher speed and intercity passenger rail projects under development plan to use freight-owned tracks and infrastructure.

B. Risk Profile

Freight rail's primary risk scenarios include sabotage to infrastructure causing the derailment of passenger trains operating on freight rail tracks; use of IEDs or Vehicle Borne Improvised Explosive Devices (VBIEDs) to cause the catastrophic release of hazardous rail cargos and/or damage to critical infrastructure; and simple attacks using small weapons or IEDs.

Passenger rail's primary risk scenarios involve loss of life from armed assaults targeting passengers in stations and on trains or degrading track structure at strategic locations that could result in a derailment.

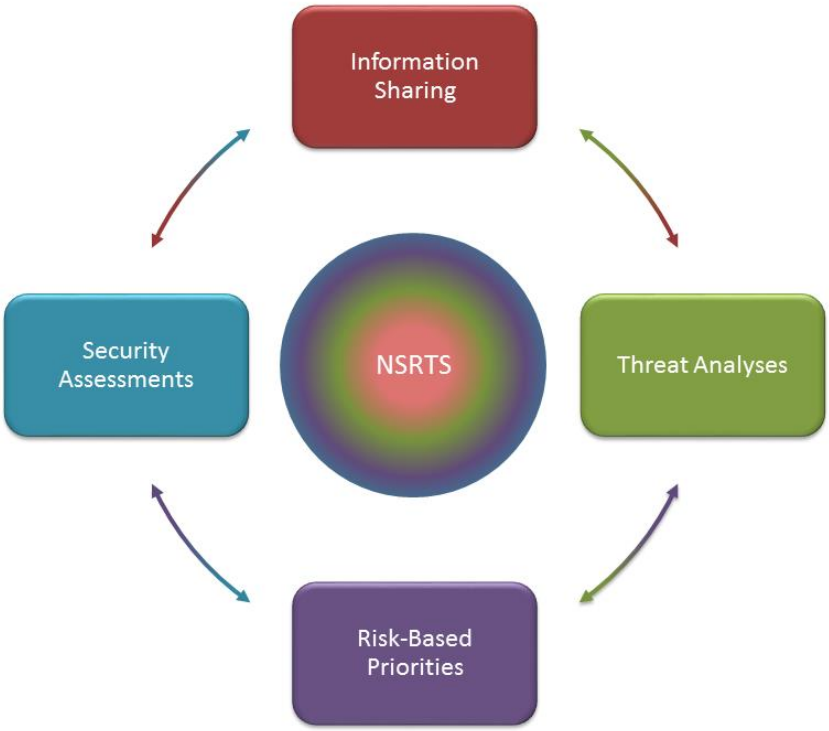
The segments of the rail network where freight and passenger operations share the same tracks are exposed to additional risk from attacks directed at people rather than property. Additionally, the general railroad system of transportation serves many vital supply chains essential for national security and commerce. Managing operational risks and the recovery of rail service relies on the resilience of the entire network for alternate routing during disruptions.

[8] Ibid.
[9] https://www.amtrak.com/national-facts. Accessed May 11, 2017.
[10] http://www.nec-commission.com/the-corridor/overview/ /. Accessed May 11, 2017.
[11] http://www.apta.com/resources/statistics/Documents/FactBook/2014-APTA-Fact-Book.pdf. 1010. Accessed December 3, 2015.

IV. Implementation

The NSRTS encourages frequent sharing of intelligence and information with freight and passenger railroad transportation owners and operators, continuous analysis and communication of threats to all transportation stakeholders, establishing risk-based priorities to ensure appropriate resourcing and administration of security measures, and assessing risks to freight and passenger railroad transportation systems through on-site security assessments and reviews. Figure 1 illustrates the high-level security activities which are necessary to operationalize the NSRTS and are detailed further in the Freight Rail Security Plan and the Mass Transit and Passenger Rail Security Plan within the NSTS.

Figure 1: Four Principal Activities Operationalizing the National Strategy for Railroad Transportation Security



A. Information Sharing

Evolving and unpredictable security threats posed to railroad transportation call for continued and relevant information and intelligence sharing between government and railroad security officials. The collaboration of railroad security partners facilitates a common understanding of threats, challenges, impacts, and feasible solutions.

The Transportation Security Administration (TSA) develops the annually updated Transportation Security Information Sharing Environment report, as required by the 9/11 Act, to "promote

sharing of transportation security information between the Department of Homeland Security (DHS) and public and private stakeholders."[12] The For Official Use report describes the process and products available for sharing pertinent threat and incident information, recommended practices, protective measures, and domain awareness updates with stakeholders.

In addition to monthly teleconferences that provide threat updates to law enforcement and security leads for freight and passenger railroads, as well as more thorough in-person consultations and coordination by officials with FBI, DHS, and DOT that occur three to four times per year, intelligence and security information is exchanged on virtually a daily basis through a variety of means implemented by government and industry. These include:

- The quarterly Freight Rail and Mass Transit Passenger Rail Government Coordinating Council and Sector Coordinating Council meetings to discuss priorities and efforts to improve security and reduce risk.
- Daily information sharing (bulletins and newsletters) for situational awareness through the Surface Transportation/Public Transportation Information Sharing and Analysis Center (ISAC).
- The Transit Policing and Security Peer Advisory Group (PAG) brings together the expertise of transit police chiefs and security directors from mass transit and passenger rail systems across North America and acts as an effective communication instrument and liaison group with TSA and other Federal Government agencies.
- The Association of American Railroads (AAR) Rail Security Working Committee is comprised of the security leads for each of the Class I freight railroads as well as several regional, short line, and passenger railroads, and manages the unified North American Railroad Industry Security Management Plan.
- The Rail Information Security Committee is the industry's cybersecurity coordination forum, and coordinates cybersecurity planning and preparedness activities.
- Security Awareness Messages, providing security information and need for heightened awareness, are developed by TSA and delivered to industry partners to encourage continued vigilance and timely reporting of suspicious incidents, reemphasize existing security measures, and/or recommend voluntary protective measures.

B. Threat Analysis

The Federal Government issues incident-specific and recurring assessments of the domestic and international threats to railroad systems. These assessments help federal, state, and local government security officials and industry professionals protect U.S. railroad systems from attacks. These products describe key terrorist actors and group ideologies, recent attacks, modes of attack, and other tactics, techniques, and procedures used by terrorists and provide a threat level based on these analyses.

[12] 49 U.S.C § 114(u).

C. Risk-Based Priorities

Seven risk-based priorities provide the foundation for supporting objectives and activities described in each of the surface modal security plans. Although the means to achieve the desired end results may vary among the different modes, the overarching vision is for TSA and its stakeholders to work together to implement programs, procedures, and processes for addressing these priorities.

The seven risk-based priorities are:

- Security planning;
- Security training;
- Security exercises;
- Critical infrastructure protection;
- Operational deterrence;
- Intelligence and security information sharing; and
- Community outreach.

D. Security Assessments

Risk assessments consider various threat scenarios and the vulnerabilities and consequences attributed to them. TSA's primary risk assessment tool is the Transportation Sector Security Risk Assessment. The process used to perform the assessment elicits detailed analyses of the vulnerabilities to and consequences of an attack (threat) on a transportation target. The results of the assessments are used to compare risks across the modes, establish risk-based priorities, and, decide on mode-specific risk mitigation actions. Other threat and risk assessments, such as DHS's National Risk Estimates, the Strategic National Risk Assessment, and modal threat assessments provide additional sources for security planning and programming decisions. These products are augmented by intelligence-driven, time-sensitive analyses of emerging events.

The Federal Government's primary method used to assess the level of security in passenger rail systems is the Baseline Assessment for Security Enhancement program. The program is designed to establish a security standard for individual system security programs and assess progress. This voluntary comprehensive review of security management focuses on multiple categories identified by the surface modal transportation communities as fundamental for a sound security program.

Using a set of industry best-practices as the benchmark, periodic voluntary program assessments on passenger rail operations provide owners and operators with information on security program gaps and the effectiveness of security plans and implementation activities. Stakeholders receive a detailed report with recommended improvements specific to their operations.

TSA also works collaboratively with freight rail operators to determine the criticality and vulnerability of strategically selected railroad infrastructure identified through the Freight Rail Critical Infrastructure assessment program. Locations and components are selected for

assessment based on a set of risk criteria including, but not limited to, the strategic value to the rail network and the co-mingling of passenger and freight rail operations. Operational assessments consisting of ground level inspections and surveys are performed to monitor and measure the level of security applied by freight rail owner/operators to Rail Security-Sensitive Materials.

In addition to Federally directed efforts, the respective North American Railroad Industry Security Committees conduct assessments annually of the industry's risk profile in physical and cybersecurity for freight and passenger railroads. These assessments are conducted as part of an annual review process established to ensure the sustained relevance and effectiveness of the industry-wide Security Management Plan. Realistic physical and cyber threat scenarios guide these assessments, which consider feasibility, adversary intent and capabilities, railroads' security posture, relevant elements of the security plan, and coordinated efforts and capabilities in implementing the plan. The results inform decisions and actions on specific provisions of the industry Security Plan and on enhancements to coordination procedures, security measures, and implementing capabilities.

E. Other Actions

Security Grant Programs

Security grant programs, including the Transit Security Grant Program, Intercity Passenger Rail Program (Amtrak), and the Intercity Bus Security Grant Program, authorized by sections 1406, 1513, and 1536 the 9/11 Act, respective, and administered by the Federal Emergency Management Agency in collaboration with TSA, directly support railroad transportation operational and capital infrastructure security activities. Security grant funds are appropriated annually, and awarded to eligible applicants to support the creation of sustainable, risk-based efforts to protect critical infrastructure and the traveling public from acts of terrorism and to increase the resilience of transportation infrastructure.

Security Regulations

Part 1580 of title 49 of the Code of Federal Regulations establishes rules for the security of rail transportation. The rules apply to passenger and freight railroad carriers that are part of the general railroad service system of transportation. The regulations require each carrier to appoint a security coordinator and report significant security concerns to TSA and for freight railroads to comply with regulations concerning location and shipping information for certain rail cars and chain of custody and control requirements.

The Hazardous Materials Regulations (Title 49, Parts 100-177) also include provisions for the security of hazardous materials in transportation. These regulations include provisions for hazardous materials carriers to have security plans and provide security awareness training for employees. Rail carriers are also required to conduct an analysis of the routes used for the transportation of Poison Inhalation Hazard materials to determine the safest and most secure route(s).

Title 49, Part 239 requires passenger railroads to have emergency preparedness plans, provide training to employees, and conduct exercises to test and validate their emergency procedures.

The 9/11 Act directs the Secretary of Homeland Security to issue regulations for a railroad security training program to prepare frontline employees to appropriately observe, assess, and report suspicious persons, activities and events. Additionally, the 9/11 Act requires railroads determined by the Secretary of Homeland Security to be at high risk for terrorism to conduct vulnerability assessments and develop comprehensive security plans. TSA is developing regulations to implement these mandates.

V. Research and Development

Transportation security and resilience is enhanced through the identification and application of existing and emerging technologies, and processes that address capability gaps. Technology enhancements lead to operational efficiencies and often reduce costs. The joint Surface Transportation Systems R&D Working Group, which includes representation from DHS, DOT, and public and private sector partners, is the primary means of identifying security capability gaps in the surface modes of transportation. The finalized capability gaps serve as a basis for developing research and development project requirements for consideration by the funding organization (e.g., DHS Science and Technology, TSA, and DOT).

VI. Performance

The Freight Rail and the Mass Transit Passenger Rail Security Plans provide outcome-based activities and measurement approaches to indicate progress in achieving NSRTS Security goals. These measures continue to be refined and developed. In some cases, data streams will need to be established to determine progress toward outcomes. Because many initiatives are voluntary, industry involvement and investment will be needed in refining outcomes, developing methodologies, and collecting data

VII. Acronyms

AAR	Association of American Railroads
DHS	Department of Homeland Security
DOT	Department of Transportation
IED	Improvised Explosive Device
ISAC	Information Sharing and Analysis Center
NSTS	National Strategy for Transportation Security
NSRTS	National Strategy for Railroad Transportation Security
PAG	Transit Policing and Security Peer Advisory Group
RAN	Railway Alert Network
RSSM	Rail Security-Sensitive Materials
TSA	Transportation Security Administration