



2020 Biennial National Strategy for Transportation Security

Report to Congress

May 29, 2020



**Homeland
Security**

Transportation Security Administration

Message from the Administrator

May 29, 2020

I am pleased to present the “2020 National Strategy for Transportation Security (NSTS),” a forward-looking, risk-based strategy designed to protect the Nation’s transportation systems from attack or disruption by terrorists or other hostile forces over the period spanning years 2020-2025. The Transportation Security Administration (TSA) prepared the NSTS pursuant to title 49 of the United States Code, section 114(s), which requires a biennial update.



TSA led the development of the NSTS, and the appended modal and intermodal security plans, with the U.S. Department of Transportation and in consultation with government and industry stakeholders. Although the NSTS is focused on counter-terrorism, TSA along with DOT, and United States Coast Guard has taken a whole-of-government approach to advance the national preparedness mission in response to the 2020 COVID-19 pandemic. All partners have continuously engaged with industry partners in the transportation systems sector to instill confidence in the return to normal operations.

In a recent audit of the 2018 NSTS, TSA concurred with the Government Accountability Office’s recommendation to better communicate with key stakeholders how the document aligns to related strategies to guide federal security efforts. TSA is committed to demonstrating how the NSTS is the governing document for federal transportation security efforts and should be used by all stakeholders in securing our Nation’s transportation system. The NSTS also aligns with other related Agency strategies and supports the strategic objectives and actions outlined in the National Cybersecurity Strategy, the National Strategy for Maritime Security and the National Strategy for Aviation Security.

TSA, as the lead federal agency for transportation security, will continue to exercise that leadership, and support federal partners both domestically and internationally, through:

- Strengthening the effectiveness of TSA’s aviation screening and in-flight security operations
- Driving improvements in aviation security through enhanced standards and robust compliance regimes
- Promoting partners’ capabilities for protecting surface transportation systems
- Enhancing passenger screening, explosives detection, credentialing, and multi-modal security in support of U.S. Coast Guard port security measures
- Expanding and improving intelligence and information sharing across mission areas
- Enhancing transportation vetting and credentialing operations
- Developing appropriate security measures and responses to counter threats to the transportation system from unmanned aircraft systems

TSA will also accomplish this by:

- Focusing on core mission areas and aligning process and technology to frontline officers
- Establishing a common view of the threat we are working to defeat

- Strengthening strategic partnerships, connections to the intelligence community, and research, analysis, and operational capabilities to mitigate potential threats
- Robust sharing of actionable information with partners
- Enhancing the fusion of known or suspected threat encounter information to provide real-time security threat awareness and drive vetting to include watch listing and screening activities

This report is being provided to the following Members of Congress:

The Honorable Roger Wicker
Chairman, Committee on Commerce, Science, and Transportation

The Honorable Maria Cantwell
Ranking Member, Committee on Commerce, Science, and Transportation

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

The Honorable Gary Peters
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 Bennie Thompson
Chairman, Committee on Homeland Security

The Honorable Mike Rogers
Ranking Member, Committee on Homeland Security

The Honorable Peter DeFazio
Chairman, Committee on Transportation and Infrastructure

The Honorable Sam Graves
Ranking Member, Committee on Transportation and Infrastructure

The Honorable Nancy P.D. Pelosi
Speaker of the House

The Honorable Steny Hoyer
House Majority Leader

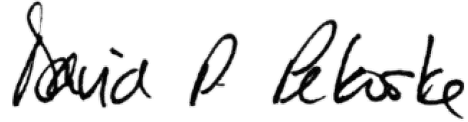
The Honorable Kevin McCarthy
House Minority Leader

The Honorable Mitch McConnell, Jr
Senate Majority Leader

The Honorable Chuck E. Schumer
Senate Minority Leader

Inquiries relating to this report may be directed to TSA's Legislative Affairs office at
(571) 227-2717.

Sincerely,

A handwritten signature in black ink, reading "David P. Pekoske". The signature is written in a cursive, flowing style.

David P. Pekoske
Administrator

Executive Summary

The 2020 National Strategy for Transportation Security 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 privacy, civil rights, and civil liberties. It identifies objectives to enhance the security of transportation infrastructure, conveyances, workers, travelers, cargo, and operations.

The strategy consists of a base plan and four security plans, including aviation, maritime, surface, and intermodal systems. The Surface strategies (National Strategy for Public Transportation Security [NSPTS] and the National Strategy for Railroad Transportation Security [NSRTS]²) that were previously annexed to the 2018 NSTS are now incorporated into the Surface modal plans. Specifically, the NSPTS was merged into the mass transit and passenger rail modal plans, and the NSRTS was merged into the freight and passenger rail modal plans.

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 ensuring 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.

¹ 49 U.S.C. § 114(s)(3)(A).

² As required by sections 1404 and 1511 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), Pub. L. 110-53 (August 3, 2007).

Strategic Environment: The strategy takes into consideration the persistent, 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 of Iraq and ash-Sham (ISIS). The strategy assumes that the targets and attack methods used overseas provide insights regarding the aspirations of adversaries domestically. Emerging terrorism risks also arise from the development of techniques or technologies that provide all adversaries with new ideas and capabilities to circumvent security measures or conduct hostile operations.

Challenges: Achieving security objectives in a resource-constrained environment requires that security managers make risk-based, cost-effective choices to secure assets and systems. The uncertainties about the adversaries’ intentions and capabilities complicate 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 privacy, civil rights, and 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 rights, and civil liberties; and the freedom of movement of people and commerce.

Risk-Based Priorities: The strategy applies a strategic risk-management approach to implement the goals.³ 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 reduce the risk of attacks.⁴ Prevention of, and protection from, historic and emerging threats requires using change management, together with knowledge management, as an enhanced approach to intelligence-driven assessments that detect attack patterns, current terrorist practices, and potential threats. Such assessments Intelligence capabilities rely on vital information sharing among transportation operators, system users, security managers, regulators, and the intelligence community. An alert and informed public provides an important force multiplier for intelligence and law enforcement efforts to prevent and respond to attacks by terrorists.

The threat of hijacking is still a concern. Attackers may also employ a variety of other 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, vehicles, knives, or a combination of weapons in single or coordinated attacks. Chemical, biological, radiological, or nuclear weapons 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 possible intrusion. Terrorists or other malicious actors, including insiders, may exploit these potential vulnerabilities to disrupt operations, finance their nefarious activities, or obtain valuable information.

Performance: 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 transportation security planning and programming:

- Enhanced use of risk-based assessments
- More effective use of information sharing products and platforms
- More effective use of security exercises
- Better understanding of the transportation resilience in supply chains
- Better understanding of cyber system vulnerabilities and consequences
- Better use of research and development initiatives to improve security effectiveness and efficiency and drive technological investment.

³ The risk-based priorities are aligned with the TSA Enterprise Risk Register.

⁴ 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.

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 on business continuity, state, local and regional preparedness, and response and recovery by transportation service providers.

The following is a synopsis of the risks outlined in the four security plans appended to the strategy. Please review each appendix for a more detailed discussion of the risks, challenges, and goals for their respective mode of transportation.

Appendix A: 2020 Aviation Security Plan

The 2020 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 actors. 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, air traffic control, and repair stations that are at the greatest risk of attack.



Appendix B: 2020 Maritime Security Plan

The 2020 Maritime Security Plan presents risk-based priorities and activities to protect the marine transportation system (MTS) from terrorism and to enhance system recovery and resilience following a terrorist incident. The goals are to save lives, preserve property, and minimize disruption to the MTS.



Appendix C: 2020 Surface Security Plan

The 2020 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 weapons, vehicle ramming, and IEDs are likely threats to the surface modes. Public transportation is particularly susceptible to attacks using standoff weapons and chemical, biological, radiological, or nuclear (CBRN) 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. Additionally, emerging technologies, such as unmanned aircraft systems, present continuing challenges to enhance procedures and capabilities to deter, detect, and prevent attacks.



Appendix D: 2020 Intermodal Transportation Security Plan

Global supply chains consist of a dense network of routes and carriers operating efficiently to provide time-sensitive deliveries. The 2020 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 national security and commerce.





2020 Biennial National Strategy for Transportation Security

Table of Contents

I.	Legislative Requirement	1
II.	Introduction.....	1
A.	Purpose and Scope.....	1
B.	Methodology	2
C.	Strategic Alignment.....	2
D.	Guiding Principles	4
E.	Strategic Environment.....	5
F.	Challenges	8
III.	Mission, Vision, Strategic Goals, and Risk-Based Priorities.....	10
A.	Goal 1: Manage Risks to Transportation Systems from Terrorist Attack and Enhance System Resilience.....	11
B.	Goal 2: Enhance Effective Domain Awareness of Transportation Systems and Threats	13
C.	Goal 3: Safeguard Privacy, Civil Rights, and Civil Liberties; and the Freedom of Movement of People and Commerce	14
IV.	Performance	15
A.	Assessing National Transportation Security Performance	15
B.	Security Program Performance Assessments	15
C.	Strategic Performance Measures	15
V.	Path Forward.....	18

VI. Transportation Operational Recovery Planning.....	20
Appendix A: 2020 Aviation Security Plan	21
Appendix B: 2020 Maritime Security Plan.....	32
Appendix C: 2020 Surface Security Plan	43
Appendix D: 2020 Intermodal Transportation Security Plan	76
Appendix E: Mandates for the Strategy.....	86
Appendix F: Supplementary Information	91

I. Legislative Requirement

The 2020 National Strategy for Transportation Security addresses requirements in legislation, executive orders, and departmental directives. See Appendix E, Mandates for the Strategy, for a full description of the statutory reporting requirements.

II. Introduction

A. Purpose and Scope

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.⁵ The strategy is developed jointly with the Department of Transportation (DOT) and submitted biennially.

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.⁶

The target audience for the strategy includes the aviation, maritime, and surface transportation communities, various Department of Homeland Security (DHS) components (Customs and Border Protection [CBP], Cybersecurity and Infrastructure Security Agency [CISA], and Countering Weapons of Mass Destruction Office [CWMD]), United States Coast Guard [USCG], as well as other government agencies (Department of State, Department of Justice, Department of Energy, Department of Defense, Department of Commerce, and the Department of Agriculture). The target audience also includes the state, local, tribal, and territorial and industry partners, as well as the traveling public and institutions of higher learning.

The desired outcome of the strategy is to inform federal partners of security activities and operations, guide the implementation of federal security programs, and promote a national unity of efforts across communities. It also seeks to ensure security operations are aligned with priorities, drive a common understanding around goals for both TSA officials and external stakeholders, and serve as a tool for communicating and coordinating with stakeholders in the Strategy, to include congressional committees. Moreover, the strategy aims to provide a whole-of-government approach for transportation security with a counterterrorism view.

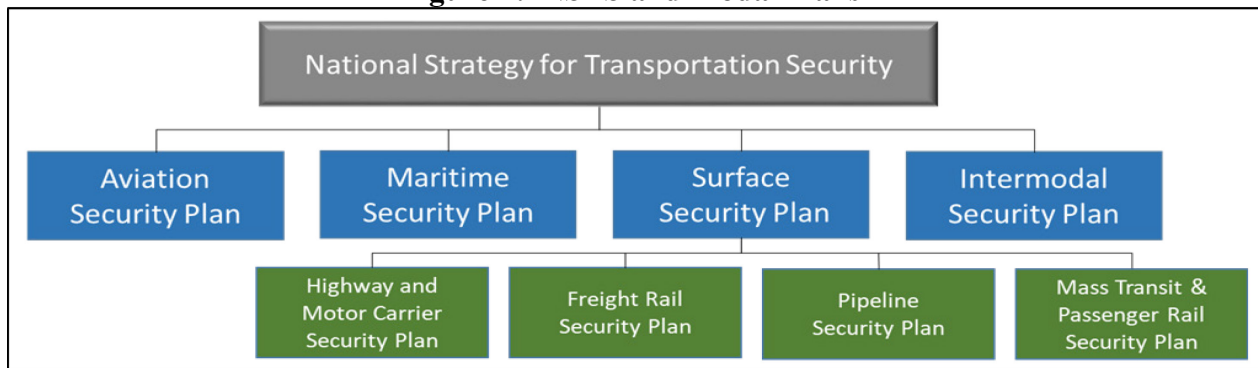
⁵ *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA), Pub. L. No. 108-458 (December 17, 2004).

⁶ 49 U.S.C. § 114(s)(3).

B. Methodology

The strategy consists of a base plan and four security plans, including aviation, maritime, surface, and intermodal systems, as illustrated in Figure 1. The Surface strategies (National Strategy for Public Transportation Security [NSPTS] and the National Strategy for Railroad Transportation Security [NSRTS]⁷) that were previously annexed to the 2018 NSTS are now incorporated into the Surface modal plans. Specifically, the NSPTS was merged into the mass transit and passenger rail modal plans, and the NSRTS was merged into the freight rail security modal plans. See Appendix F, Supplemental Information, for a full description of methodology used to develop the strategy and modal security plans.

Figure 1: NSTS and Modal Plans



C. Strategic Alignment

There are a number of current strategic national and departmental plans addressing counterterrorism. The NSTS incorporates, to the greatest extent possible, the missions and objectives of those strategies and plans as they pertain to the protection of transportation systems, infrastructure, cargo, mail, baggage, travelers, workers, and conveyances.

While the strategy is intended to serve as 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 (see Appendix F, Supplemental Information, for roles and responsibilities).⁸ The strategy builds on the demonstrated commitment of the transportation industries to continually advance security programs through the most appropriate, practical, and cost-effective means. It provides input into other TSA strategic documents and operations plans such as TSA's Crosscutting Risk-Based Security Strategy and TSA's Strategy for Surface Transportation Security Inspectors Operations Plan (as shown in Figure 2). Moreover, it supports the strategic objectives and actions outlined in the National Cybersecurity Strategy, National Cyber Strategy Implementation Plan, National Cyber Incident Response Plan, National Strategy for Maritime Security, and the National

⁷ As required by sections 1404 and 1511 of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (9/11 Act), Pub. L. 110-53 (August 3, 2007).

⁸ 49 U.S.C. § 114(s)(5) and (6).

Strategy for Aviation Security.⁹ This strategy is not intended to replace agency strategies or planning documents related to transportation security, however, it is intended to guide efforts within this space.

Figure 2: 2020 NSTS Strategic Alignment

2020 NSTS	STRATEGIC DOCUMENT	STRATEGIC ALIGNMENT
✓	TSA Crosscutting Risk-Based Strategy	Aligned with associated goals and objectives to guide TSA's risk-based priorities and activities across aviation and surface transportation modes.
✓	TSA Cybersecurity Roadmap	Cybersecurity risks within the transportation systems sector will be assessed and included in the NSTS.
✓	TSA Strategy for Surface Transportation Security Inspectors Operations Plan	Establish Transportation Security Inspector-Surface operational priorities and activities conducted with surface transportation stakeholders.
✓	Surface Transportation Risk-Based Security Strategy	Aligned with associated goals, objectives, activities, outcomes, and performance measures to guide TSA's mitigation of surface vulnerabilities and risks.

⁹ The seven supporting plans of the NSAS include: Aviation Operational Threat Response Plan (AOTR), Aviation Transportation System Security Plan (ATSS), Aviation Transportation System Recovery Plan (ATSR), Aviation Domain Awareness and Intelligence Integration Plan (ADAIL), International MANPADS Threat Reduction Plan (IMTR), Domestic Outreach Plan (DO), and International Outreach Plan (IO).

D. Guiding Principles

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



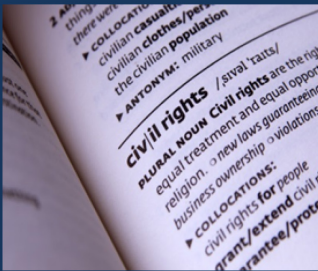
Intelligence-Driven, Risk-Based Approach

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, Civil Rights, and Civil Liberties

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.

E. 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 commerce.¹⁰ 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 and related public spaces serving major urban areas; air cargo systems; strategic and commercially important seaports and waterways; and highways, tracks, tunnels, bridges, rolling stocks, 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, attacks at domestic airports and a number of disrupted plots and attacks across the country show that terrorists are persistent, dynamic, and adaptive. The strategy takes into consideration the evolving nature of terrorist threats and the challenges posed by a more dispersed and less visible enemy (such as a lone offender who is motivated by one or more violent extremist ideologies who, operating alone, supports or engages in

On June 21, 2017, Canadian national Amor M. Ftouhi entered Bishop International Airport (FNT) in Flint, Michigan, and stabbed a police officer in the neck with a knife. Ftouhi referenced killings in Syria, Iraq, and Afghanistan as a justification for his actions.

¹⁰ 49 U.S.C. § 114(s)(3)(A).

acts of unlawful violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor.). To address this dynamic threat, the strategy is 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. Aviation specifically is a preferred target for terrorists seeking to conduct spectacular mass-casualty attacks that cause economic damage and garner widespread media attention. ISIS, al-Qa'ida, and its affiliates have all been involved in conducting or plotting aviation attacks and probably have the greatest capability to carry out attacks against United States or Western airlines. IEDs remain the preferred tactic for aviation attacks and terrorist groups will almost certainly continue to develop innovative tactics and concealment techniques to try to get bombs onboard aircraft. Recent terrorist aviation attacks have also targeted ground-based aviation infrastructure using a variety of tactics, including small arms and suicide bombings.

U.S. Maritime Critical Infrastructure has been assessed by the United States (U.S.) Office of Secretary of Defense for Homeland and Global Security to be a contested environment because the U.S. Homeland physical and cyberspace domains are not fully controlled by the U.S. Due to U.S. conventional supremacy and overmatch for near peer adversaries, many adversary operations have been driven to operate in the “gray zone” against soft targets, predominately targeting U.S. critical infrastructure. Gray zone operations are designed to degrade, deter, and deny the U.S. achievement of strategic goals through in-direct (non-contact) actions, including cyber-operations, short of war.

Surface transportation systems—to include mass transit passenger rail, freight rail, pipelines, and highway motor carriers—remain a target of interest to domestic threat actors. Internationally, terrorist groups continue to promote and conduct attacks on surface transportation targets, specifically placing increased emphasis on conducting vehicle-ramming attacks in their propaganda.

International threats to transportation are predominantly associated with transnational terrorist organizations, such as ISIS and al-Qa'ida. Overseas attacks indicate aviation, public transportation, including ferries, over-the-road buses, and pipeline assets as likely targets. Increasingly, terrorist tactics involve single individuals or small teams of adversaries to orchestrate attacks on 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 are newly discovered risks that are evolving in unexpected ways with unanticipated consequences as well as risks that already exist. They 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 the demonstrated use of UAS to attack critical infrastructure overseas or to disrupt airport operations, as seen at Gatwick Airport

in December 2018, raise the specter of such an attack or disruption domestically.¹¹ Terrorists continue to develop and deploy innovative concealment methods, as exemplified by the use of laptops to conceal explosives.

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; Barcelona and Cambrils, Spain; and New York City—reveal an emerging threat encouraged by terrorist messaging.

Our adversaries and strategic competitors have cyber-attack capabilities they could use against U.S. critical infrastructure, including U.S. transportation 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.

In April 2017, a suicide attacker detonated an IED on a metro passenger car traveling between stops in St. Petersburg, Russia, resulting in 15 killed, including the attacker, and more than 100 wounded. A second IED was found and diffused at a separate metro station.

In July 2017, Australian authorities disrupted a plot to smuggle an IED concealed in a meat grinder onto a commercial aircraft traveling from Sydney to Abu Dhabi.

In September 2017, an attacker detonated an IED inside a crowded subway car during the morning rush hour at Parsons Green station in West London, UK, injuring 29 people.

In March 2019, a school bus driver hijacked a school bus with 51 children aboard near Milan, Italy. The driver rammed the school bus into police cars and then set the bus on fire, injuring 14.

¹¹ 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. *See* 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 (in 49 U.S.C. § 44801(9), is an unmanned aircraft weighing less than 55 pounds)), including the weight of anything attached to or carried by the aircraft. In addition, 49 U.S.C. 44801(12) defines an unmanned aircraft as an aircraft that is operated without the possibility of direct human intervention from within or on the aircraft, without regard to weight.

While there have been few incidents of chemical, biological, radiological, or nuclear attacks domestically, due to the growing accessibility of the underlying technologies associated with the use of chemical, biological, radiological, and nuclear agents as weapons, these threats also present a significant future risk.

F. 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 can be 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 and owner / operator 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 programming is informed by strategic planning, it is also a tool for policy implementation, accountability, and performance. Annual funding requests 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 DHS, Federal Emergency Management Agency (FEMA), and DOT. 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. It 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 assessing baseline risk and the effectiveness of specific initiatives equitably across all transportation services. 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, as well response efforts. The recovery of transportation services following an attack is dependent on the resilience of the systems and 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**

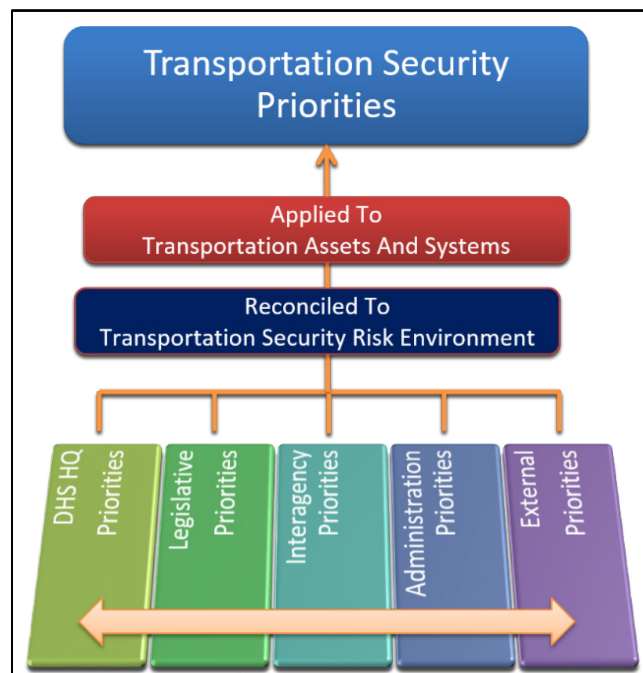
III. Mission, Vision, Strategic Goals, and Risk-Based Priorities

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 privacy, civil rights, and civil liberties.

Figure 3 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 spans the preparedness mission areas. These risk-based priorities align with the TSA Enterprise Risk Register and are further developed in the modal security plans.

Figure 3: Development of Risk-Based Priorities



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 materials or devices 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. As appropriate, transportation system operations will include Global Nuclear Detection Architecture (GNDA) planning, cooperation, and collaboration efforts pursuant to the SAFE Port Act.¹²

Risk-Based Priority 3: Cybersecurity

Cybersecurity risks vary across the transportation modes. Commercially available tools enable threat actors to hack into business networks or ICS to compromise the safety of transportation operations. The strategy encourages system owners and operators to assess the threats to their cyber systems and, where possible, collaborate across the public and private sectors to research defensive measures and invest appropriately to secure them.

Risk-Based Priority 4: Preventing Terrorist Travel

Preventing terrorist travel is a top priority. The strategic approach to preventing terrorist travel across the transportation system relies on the intelligence, security, and law enforcement communities working together to identify, detect, deter, or interdict terrorist travel. The strategy emphasizes screening and vetting countermeasures. Screening describes the process that may include, but is not limited to, government officials searching for available information on an individual in various databases. Vetting describes the combined automated and manual processes used to match an individual's information against threat factors and known derogatory information in an effort to

¹² 6 U.S.C. 596a § 1907.

determine potential risk. Vetting includes automated biographic and/or biometric matching against watchlists and threat information as well as manual and automated processes used to resolve potential matches and false positives.¹³

Risk-Based Priority 5: Insider Threats

Attacks may be conducted or facilitated by insiders within the transportation workforce. This includes workers employed by transportation companies, on-site vendors, or contract personnel who, wittingly or unwittingly, supply information to unauthorized individuals or execute an attack. The strategy emphasizes countermeasures to improve vetting capabilities, personnel security assessments, and credentialing programs. TSA is also implementing recommendations provided by the GAO¹⁴ and Aviation Security Advisory Committee Insider Threat Subcommittee to mitigate the insider threat to aviation security.

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 6: 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, state, local, tribal, and territorial 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 terrorists or other hostile actors, 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.¹⁵

¹³ National Strategy to Combat Terrorist Travel, pp 14 & 15. www.whitehouse.gov/wp-content/uploads/2019/02/NSCTT-Signed.pdf.

¹⁴ <https://www.gao.gov/assets/710/704443.pdf>.

¹⁵ 6 U.S.C. § 942.

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

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.”¹⁶ 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.

“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.

Through domain awareness, security personnel are better able to understand threats and manage security risks within the scope of their functions and responsibilities.

Risk-Based Priority 1: Assessments

An initial step to managing security risks across all modes is to understand how transportation assets, systems, and networks may be attacked. TSA and the United States intelligence community assess 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 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 personally identifiable information and other sensitive information is appropriately safeguarded and that accurate, pertinent information flows quickly to operators, government, public safety and security officials, and the public.

¹⁶ Air and Marine Operations Vision 2025, p. 12.

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 threats.

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

Managing risk, enhancing resilience, and effective domain awareness depend on our ability to safeguard and protect privacy, civil rights, and 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 Civil Liberties During Screening

The security screening process must respect the unique personal circumstances of travelers and protect their civil rights and civil 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 data systems. Government and industry must apply strict security protocols to protect sensitive information. New technologies that promote open data access must be assessed for potential threats to existing protocols for maintaining the security of the transportation system.

IV. Performance

A. Assessing National Transportation Security Performance

Federal, state, local, tribal, and territorial government levels as well as 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. 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 physical and cybersecurity infrastructure provide the primary means to understand the elements of risks, develop risk-based priorities, and determine progress in 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. Airport perimeter security 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 associated 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: TSA's Transportation Sector Security Risk Assessment (TSSRA) and the USCG Maritime Security Risk Analysis Model (MSRAM).

C. Priority Outcomes

The modal security plans provide metrics for key activities indicating the progress managing priority risks in each mode. Figure 4 identifies the outcomes for the strategic priorities for each goal as identified in the modal plans.

¹⁷ 49 U.S.C. § 114(s)(4)(B).

Figure 4: Performance Outcomes

NSTS Goal	Risk-Based Priority	Outcome
<p>Manage risks to transportation systems from terrorist attack and enhance system resilience.</p>	<ul style="list-style-type: none"> • Physical Security • Weapon Detection Programs • Cybersecurity • Preventing Terrorist Travel • Insider Threat • Preparedness 	<p>Perimeters of sensitive transportation locations are not breached by terrorists.</p> <p>Critical transportation infrastructure is secure and resilient against terrorist attacks.</p> <p>Dangerous articles are not introduced into the transportation systems.</p> <p>Weapons of mass destruction (WMDs) are not carried in commercial transportation.</p> <p>Chemical and biological threats are detected and neutralized.</p> <p>Information systems vital to the safe, secure, and efficient operation of transportation systems are protected from malicious cyber activity.</p> <p>Terrorists are not able to travel by commercial aviation.</p> <p>Terrorists do not enter the United States.</p> <p>Transportation system employees in security sensitive positions are vetted to minimize insider threat risks.</p> <p>Transportation systems and conveyances are not used as weapons of mass consequence (for example, bulk containers of toxic, flammable, or explosive materials are not used as weapons).</p>
<p>Enhance effective domain awareness of transportation systems and threats.</p>	<ul style="list-style-type: none"> • Assessments • Information Sharing • Situational Awareness, Common Operating Picture • Training 	<p>High-risk transportation assets and systems that must be protected undergo routine and recurrent assessments to determine progress in mitigating new and previously identified vulnerabilities.</p> <p>Transportation stakeholders are satisfied with intelligence-related and other security information shared.</p> <p>Emergency responders and stakeholders have satisfactory access to the common operating picture.</p> <p>Exercise and training services build operational capacity through domain awareness and application of best practices.</p>

NSTS Goal	Risk-Based Priority	Outcome
<p>Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce.</p>	<ul style="list-style-type: none"> • Accelerated Screening of Low-Risk Passengers and Cargo • Protecting Civil Rights and Civil Liberties during Screening • Protecting Sensitive Information 	<p>Enrollment in TSA Pre✓® program and related programs is increased.</p> <p>The DHS Traveler Redress Inquiry Program (TRIP) is available to travelers and cases are processed timely.</p> <p>Passenger screening time remains within approved standards for screening, based on type.</p> <p>Enrollment in Customs-Trade Partnership Against Terrorism (CTPAT) and related programs is increased.</p> <p>Cargo delays are minimized.</p> <p>The screening of travelers with special needs is facilitated.</p> <p>New technologies for systems that maintain sensitive information are assessed for threats.</p>

V. Path Forward

The security responsibility of the Nation's transportation systems is shared among multiple jurisdictions at federal, state, local, tribal, and territorial government levels and with public and private transportation owners and operators. Consequently, the management of security risks depends 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, as well as cyber 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 sharing 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 sharing 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 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 resiliency and reliable delivery of goods over transportation systems through intermodal connections and transshipment points. For example, U.S. overreliance on products manufactured and delivered from abroad, or state-controlled manufacturers and suppliers, present potential resiliency and reliability vulnerabilities. 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 and must be protected from non-kinetic threats such as those presented by cybersecurity vulnerabilities. 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, as well as the nation's defense mission.

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 and capabilities 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.

The following are the research and development (R&D) priorities (not in prioritized order):

- Anomaly/explosives detection
- 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
- Interoperable information systems
- Chemical, biological, radiological, and nuclear threat security
- Detect, track and identify, mitigate UAS threat, and
- Remote area detection

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, including responses to natural and human-caused disasters and terrorist 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 links transportation recovery processes with the principles found in the National Preparedness System, the National Response Framework, and the National Disaster Recovery Framework.¹⁸ 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 response and 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.²⁰ These organizations plan for all aspects of transportation operations and infrastructure projects, including response and recovery from emergencies.

The *Stafford Disaster Relief and Emergency Assistance Act* provides an orderly and continuing means of assistance by the Federal Government to state and local governments in carrying out their responsibilities to alleviate the suffering and damage that result from disasters. For example, it provides federal assistance programs for both public and private losses sustained in disasters. Specifically, these programs use services of all appropriate agencies to assist in developing disaster preparedness plans for mitigating, warning, emergency operations, rehabilitation, and recovery; training and exercises; post disaster critiques and evaluations; annual review of programs; coordination of federal, state, and local preparedness programs; application of science and technology; and research.²¹

¹⁸www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE_Final%20Version_08-27-2014.pdf.

¹⁹www.transportation.gov/disaster-recovery.

²⁰ 49 U.S.C. 5303.

²¹ www.fema.gov/media-library/assets/documents/15271. *Stafford Disaster Relief and Emergency Assistance Act*, February 23, 2018. (Pub. L. 100-707).



Appendix A: 2020 Aviation Security Plan



**Homeland
Security**

Transportation Security Administration

2020 Aviation Security Plan

I. Introduction

A. Overview

The 2020 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.²² Within these components, there are many aviation support functions and activities providing services as defined in the aviation ecosystem.²³ Aircraft maintenance, airport concessions, fuel services, ground maintenance and repair services, and food and drink vendors exemplify the extended community included in the aviation ecosystem.

Additionally, the ATS community must address the challenges of securing the aviation ecosystem from the emerging threats posed by malicious cyber activity and both errant and malicious use of UAS. Any disruption of critical infrastructure elements in the aviation domain could create ripple effects throughout the entire system. Securing the aviation domain and its ecosystem requires collaboration with industry and interagency partners to effectively manage and mitigate risks to the system. The interagency community is actively working to promote the safe and secure integration of UAS into the national airspace system.

This Aviation Security Plan implements National Security Policy Directive 47/Homeland Security Policy Directive 16, Aviation Security Policy by continuing the enhancement of U.S. homeland and national security by protecting the United States and its interests from threats in the aviation domain and its ecosystem.^{24,25} It also provides a strategic approach to securing both the aviation domain and its ecosystem from terrorist attacks and advances the goals of the strategy by identifying objectives and activities.

1) Modal Profile

In the interest of national security and commerce, aviation assets and systems that need to be protected from attack by terrorists include, but are not limited to: the air traffic control system, domestic airports, foreign airports serving as the last-points-of departure for the United States, commercial airliners and cargo aircraft operating in, to, and from the United States, general

²² 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” NSPD-47/HSPD-16.”

²³ The term “aviation ecosystem” is an extensive multi-layered network of intersecting elements with integral roles in aviation domain and involves six primary entities: airports, airlines, airlift, actors, and aviation management. The National Airspace System falls under aviation management within the aviation ecosystem.

²⁴ NSPD-47/HSPD-16.

²⁵ 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), 2018.

2020 Aviation Security Plan

aviation aircraft, airports operating under TSA’s security programs, air cargo and aircraft maintenance industries, and flight schools.²⁶

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

The components in Figure 5 identify the main sub-modal aviation communities and the organizational approach to security planning and programming.²⁷

Figure 5: 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 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. Certain private charter operations are also deemed commercial flights.
Commercial Airports	Commercial service airports are defined as public airports that have at least 2,500 passenger boardings per year and have scheduled passenger service. ²⁸ There are approximately 440 ²⁹ airports in the United States that have airport security programs. TSA assesses certain non-U.S. airports to satisfy statutory requirements and determine compliance with security-related International Civil Aviation Organization Standards and Recommended Practices.
General Aviation	General aviation is defined as aircraft operation for personal, recreational, or other noncommercial (any flights not accepting money for passenger or cargo) purposes. 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.
Air Traffic Control	Air traffic control is a service provided by ground-based air traffic controllers who direct aircraft on the ground and through controlled airspace, and can provide advisory services to aircraft in non-controlled airspace. The primary purpose of air traffic control worldwide is to prevent collisions, organize and expedite the flow of air traffic, and provide information and other support for pilots.
Repair Stations	Foreign and domestic repair stations inspect, repair, replace, or overhaul aviation products and articles, including airframes, engines, propellers, and radios among others.

²⁶ Flight schools are a potential source of training for terrorists, who might then misuse that training to conduct attacks.

²⁷ The components of the aviation mode incorporate the protection of the aviation ecosystem.

²⁸ Title 49 U.S.C. 47102(7).

²⁹ Numbers fluctuate due to seasonality.

2020 Aviation Security Plan

2) Risk Profile

The risk profile for the aviation mode of transportation is dominated by international terrorism, but also includes domestic terrorism.³⁰ The greatest threat to aviation security remains explosives, especially non-metallic IEDs. New and emerging technologies, such as UAS and 3D printing technology, provide opportunities for terrorists to attack aviation targets in ways that are difficult to detect.

International and Domestic Terrorists: Terrorist attacks on transportation assets frequently involve the deployment of IEDs on a person, in cargo or baggage, or in a vehicle. Aircraft may be used as weapons of mass destruction, or may transport CBRN materials in cargo, in addition to IED components or other terrorist material. Travelers at intermodal aviation and transit venues are exposed to other types of attacks due to open and congested public areas, such as vehicle ramming or VBIED attacks in areas with adjacent, public roadways. The public areas allow attackers access to occupied assembly areas for ticketing, baggage pick-up, and screening. Terrorists acting alone or in small units can gain access to crowded terminals to perpetrate attacks using explosives, small arms, edged weapons, or CBRN weapons and materials.

An on-going security concern is the potential for individuals within the United States to radicalize, or otherwise become motivated to violence, and attack transportation assets. Terrorist organizations openly incite—through videos, magazines, and online forums—sympathizers in the United States to commit acts of violence. The risk posed by these U.S.-based 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 other countries, link up with terrorist organizations, receive training and operational experience, and return to the United States with a terrorist purpose. Racially or ethnically motivated violent actors, who may or may not have transnational linkages, represent a segment of domestic terrorism and may target assets in the aviation ecosystem.

Insider Threats: Individuals holding trusted positions and having access to sensitive information or locations who are willing to commit malicious acts are often more difficult to detect. Malicious insiders may facilitate cyber or physical attacks by others or act independently; unwitting employees may facilitate such attacks inadvertently.

UAS: UAS, often referred to as drones, are used for a growing variety of government, business, research, and recreational purposes, and the associated technology is evolving rapidly; however, terrorists may also employ them for delivery of ordnance or to otherwise facilitate terrorist activities. While most operators are pursuing legitimate activity, the risk of a malicious actor using UAS for nefarious ends is increasing. UAS are easily obtained and could be used to deliver a lethal payload of explosives or CBRN agents with little opportunity for interdiction. They 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

³⁰ Risk profiles and scenarios sources include TSSRA and TSA aviation assessments.

2020 Aviation Security Plan

UAS attack or activity by misguided/misinformed individual might be small, a coordinated attack by several could have a major impact.

The risk profiles listed in Figure 6, informed by TSSRA and other intelligence analyses, provide the basis for risk-based aviation security priorities.

Figure 6: 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. In addition, cargo may be used to facilitate the transfer of components or material as part of attack planning against other sectors.
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, the use of aircraft as weapons, 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 to commercial airlines, security risks remain elevated due to persistent attempts by terrorists to thwart security measures. Terrorists also seek to transit via the commercial airline sector.
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. Air traffic control facilities, whether on or off airport property, are at risk of being compromised when actors gain access to a control center and direct aircraft to collide into each other. Furthermore, the air traffic control may be disrupted through physical attacks (for example, vehicle IED) to a facility. Terrorist attacks may also be facilitated by insiders, wittingly or unwittingly, providing information or access needed to execute an attack. Unidentified drone activity in key airport locations could have cause an outsized disruption to airport traffic.
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.
Flight Schools Risk Profile	Flight schools are vulnerable to exploitation by attackers seeking to acquire pilot skills and access to aircraft. U.S. flight schools' enrollment practices are governed in Transportation Security Regulations and establish student vetting and reporting requirements for flight schools.

2020 Aviation Security Plan

Repair Station Risk Profile

Repair stations are vulnerable to insider exploitation, which may include aviation maintenance workers, for attacks using sabotage, or threat items placed on aircraft. Most repair stations are within the perimeter of an airport, but some are off-airport, or on the perimeter itself (that is, operating with public side and airside, similar to most cargo facilities). The Federal Aviation Administration (FAA) establishes aviation safety requirements for repair stations in title 14 of the Code of Federal Regulations (CFR), part 145 (Repair Stations). For security matters, repair stations are required to comply with 49 CFR part 1554: Aircraft Repair Station Security.

B. Risk-Based Priorities

Aviation analysts review data from intelligence reports, security assessments and inspections, exercises, and incident reports to identify threats or vulnerabilities, develop risk management strategies, and establish program priorities. The following risk-based priorities for the aviation mode come 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 in regulatory inspections, threat and vulnerability assessments, and risk analyses using sound security principles.

Screening Technology: Screening technology used by federal agencies and private industry detects and prevents the introduction of weapons or other lethal agents into transportation venues. Screening and advance information technologies to mitigate the risk of introducing TSA prohibited items into the ATS whether carried on a person, in baggage, or in cargo.

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

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, as appropriate.

2020 Aviation Security Plan

Insider Threat: Attacks may be conducted or facilitated by insiders within the transportation workforce. This includes workers employed by transportation companies, on-site vendors, or contract personnel who, wittingly or unwittingly, supply information to unauthorized individuals or execute an attack. The strategy emphasizes countermeasures to improve vetting capabilities, personnel security assessments, and credentialing programs.

Preventing Terrorist Travel: Preventing terrorist travel is a top priority. The strategic approach to preventing terrorist travel across the transportation system relies on the intelligence, security, and law enforcement communities working together to identify, detect, deter, or interdict terrorist travel. The strategy emphasizes screening and vetting countermeasures. Screening describes the process that may include, but is not limited to, government officials searching for available information on an individual in various databases. Vetting describes the combined automated and manual processes used to match an individual's information against threat factors and known derogatory information in an effort to determine potential risk.³¹

Protecting Privacy, Civil Rights, and Civil Liberties during Screening: The security screening process must respect the unique personal circumstances of travelers and protect their privacy, civil rights and civil liberties. Federal Government and private-security service providers should 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. Expedited screening of low-risk populations can be translated directly to more effective deployment of screening resources for higher-risk populations. However, unrestricted mobility presents unacceptable risks in the present threat environment. Security officials determine the necessary level of screening by making risk-based decisions and evaluating the risks associated with travelers and cargo by applying technologies, data sources, and analytical methods.

Cybersecurity: Cybersecurity protocols should be employed to defend, monitor, and stabilize information technology-based, mission-critical systems, such as access controls; closed circuit television and other surveillance systems; telecommunications; operations/command centers; and industrial control systems/SCADA systems used for electricity, fuel delivery, climate controls (such as heating, ventilation, and air conditioning systems), air traffic control systems, and water/waste water systems.

³¹ National Strategy to Combat Terrorist Travel, pp 14 & 15. www.whitehouse.gov/wp-content/uploads/2019/02/NSCTT-Signed.pdf.

2020 Aviation Security Plan

II. Objectives, Activities, and Measuring Progress

The 2020 Aviation Security Plan’s goals and objectives reflect the risk-based priorities. Figure 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 aviation security. This approach makes clear that no one government or agency can carry out a national security mission independently.

Figure 7: Aviation Security Goals

NSTS Goal 1	Manage risks to ATS from terrorist attacks and enhance system resilience
Objective 1.1: Improve physical and cybersecurity of domestic aviation critical infrastructure.	<p>Activity 1.1.1: Increase the number of aviation workers requiring a fingerprint-based criminal history records check and increase the use of Rap Back for recurrent criminal vetting of workers requiring unescorted access to non-public areas of airports. (TSA and Federal Bureau of Investigation [FBI])³²</p> <p>Outcome: Reduction in vulnerability to potential insider threats from aviation workers.</p> <p>Performance Measurement: Percentage of aviation workers receiving recurrent vetting through Rap Back who must have a criminal history records check to have unescorted access to non-public areas of airports. (DHS/TSA)</p>
	<p>Activity 1.1.2: Assess cybersecurity vulnerabilities of commercial aircraft and airports survey. (Cybersecurity and Infrastructure Security Agency [CISA], TSA, and FAA)</p> <p>Outcome: Identify cyber vulnerabilities that may affect safe operation of commercial aircraft to support the FAA’s, aircraft and other aviation manufacturers’, aircraft operators’, and airport operators’ analysis of potential risks to safety of flight and the development of appropriate mitigation measures, as needed.</p> <p>Performance Measurement: Percentage of organizations that have implemented at least one aviation cybersecurity enhancement after receiving a vulnerability assessment or survey. (CISA and TSA)</p>
	<p>Activity 1.1.3: Assess UAS risk in the environs of commercial airports. (DHS/TSA/DOT/FAA)</p> <p>Outcome: Identify, track, report, and mitigate UAS threats and vulnerabilities affecting safe operations at commercial airports.</p>

³² The Rap Back service allows authorized agencies to receive notification of activity on individuals who hold positions of trust (for example, 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. www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi, accessed February 1, 2018. TSA already performs recurrent vetting for ties to terrorism. Rap Back provides recurrent criminal vetting capability.

2020 Aviation Security Plan

NSTS Goal 1	Manage risks to ATS from terrorist attacks and enhance system resilience
	<p>Performance Measurement: Percentage of Joint Vulnerability Assessments (JVAs) conducted at commercial airports having resulted in implementing at least one UAS risk mitigation countermeasure. (DHS/TSA)</p>
<p>Objective 1.2: Improve capabilities to prevent, protect, mitigate, respond to, and recover from terrorist attacks throughout the aviation community.</p>	<p>Activity 1.2.1: Strengthen technical skill of frontline employees to identify, deter, prevent, and respond to threats to the homeland by expanding training and development programs and security awareness messaging describing common threat indicators. (DHS/TSA and industry)</p> <p>Outcome: Dangerous articles are not introduced into the aviation system.</p> <p>Performance Measurement: Track system effectiveness using covert testing test results to identify trends and vulnerabilities over time. (DHS/TSA)</p>
<p>Objective 1.3: Enhance international aviation security risk management strategies.</p>	<p>Activity 1.3.1: Conduct outreach to facilitate the use of international best practices and procedures. (U.S. Department of Justice/Federal Bureau of Investigation, DHS/CBP/TSA, DOT/FAA, and U.S. Department of State)</p> <p>Outcome: International policies and aviation security programs support U.S./DHS objectives of raising the baseline of global aviation security.</p> <p>Performance Measurement: Percent of foreign last point of departure airports where TSA has taken action to raise the global baseline. Actions could include, but are not limited to, the installation of new technology (such as Computed Tomography), covert testing collaboration (to include joint covert testing), the use of canine teams authorized by the host government, implementation of a national Man-Portable Air Defense Systems mitigation strategy, FAMS agreements, and collaboration with DHS towards becoming preclearance airports. (DHS/TSA)</p> <p>-----</p> <p>Activity 1.3.2: Assess compliance with security measures required for service to the United States. (DHS/CBP/TSA)</p> <p>Outcome: Identify compliance or noncompliance with security measures required for service to the United States.</p> <p>Performance Measurement: Percentage of aviation security vulnerabilities which are closed through assessment and inspection activities. (DHS/TSA)</p> <p>-----</p> <p>Activity 1.3.3: Scan international inbound air cargo shipments entering the United States to detect radiological or nuclear threats. (DHS/CBP/CWMD)</p> <p>Outcome: Reduction of the risk of illicit radiological or nuclear agents entering the United States.</p> <p>Performance Measurement: Percent of international air cargo, including special express commercial services cargo and mail, which passes through radiation detection systems upon entering the Nation at ports of entry. (DHS/CBP)</p>

2020 Aviation Security Plan

NSTS Goal 1	Manage risks to ATS from terrorist attacks and enhance system resilience
Objective 1.4: Increase security technology capability to respond to known and emerging threats.	<p>Activity 1.4.1: Leveraging TSA work to harmonize standards internationally and improve aviation industry stakeholder participation in the R&D process for threat detection and screening capabilities. (DOT, DHS/ Science and Technology Directorate/TSA, U.S. Department of State, R&D community, and industry)</p> <p>Outcome: Increased aviation industry stakeholder participation in processes to identify security capability gaps and develop solutions on a global scale.</p> <p>Performance Measurement: Percentage of aviation industry stakeholder participation in the R&D process to raise global detection and screening capabilities. (DHS/TSA)</p>
NSTS Goal 2	Enhance effective aviation domain awareness of transportation systems and threats³³
Objective 2.1: Improve quality in the sharing of intelligence information and products for government, industry, and public awareness.	<p>Activity 2.1.1: Enhance the quality and applicability of intelligence sharing with security partners. (DHS/TSA and industry)</p> <p>Outcome: Improved quality and applicability of intelligence shared with customers.</p> <p>Performance Measurement: Percentage of annual customer surveys indicating TSA intelligence information helps the customer organization accomplish its mission and objectives. (DHS/TSA)</p>
NSTS Goal 3	Safeguard privacy, civil rights, civil liberties, and the freedom of movement of people and commerce
Objective 3.1: Apply risk-based security approach to supply chain and passengers.	<p>Activity 3.1.1: Resolve security risks of high-risk cargo identified by the Air Cargo Advance Screening program, by screening all inbound air cargo shipments prior to loading onto aircraft destined for the United States. (DHS/CBP and DHS/TSA)</p> <p>Outcome: Enhanced freedom of movement of low-risk cargo.</p> <p>Performance Measurement: Percentage of cargo shipments targeted by Air Cargo Advance Screening that returned a Referral for Screening (RFS), which would require that TSA apply enhanced screening measures. (DHS/TSA)</p> <p>-----</p> <p>Activity 3.1.2: Provide expedited aviation security screening for trusted travelers. (DHS/CBP and DHS/TSA)</p> <p>Outcome: Expedite low-risk travelers through security screening programs and enhance legitimate traveler experience and continue to explore options to achieve greater efficiencies in TSA Pre✓® and Global Entry programs, and DHS TRIP.</p> <p>Performance Measurement: Percentage of daily passengers receiving expedited screening based on assessed low risk. (DHS/TSA)</p>

³³ NSAS, 2018.

2020 Aviation Security Plan

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 as quickly as possible following a disruption.

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 on the aviation ecosystem, as well as measures that will enable the ATS and other affected critical government and private sector aviation-related elements to recover from such an attack as rapidly as possible.”³⁴

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. The range of incidents may include scenarios identified in the Aviation Risk Profile.

Title 49 CFR 1542.103 requires airports to have a security program, and 49 CFR 1542.307 requires airports to have incident management procedures to address incidents or threats and to review their incident management 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.

³⁴ Aviation Transportation System Recovery Plan, 2018.



Appendix B: 2020 Maritime Security Plan



**Homeland
Security**

Transportation Security Administration

2020 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 2020 Maritime Security Plan addresses the security of maritime assets that must be protected from terrorist attacks, including cyber-related 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: to save lives, preserve property, minimize disruption to the MTS and the maritime community, and protect the environment. The public and private sectors 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; state, local, tribal, and territorial government agencies; waterway users; industry; NGOs, philanthropics, academia, foreign governments; and international operators are vital partners in the collaborative effort to secure the system and ensure its resilience.

3) Modal Profile

The MTS is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports.³⁵ It supports \$5.4 trillion dollars of economic activity each year and accounts for the employment of more than 30 million Americans.³⁶ The maritime transportation of cargo is considered the most economical, environmentally friendly, and efficient mode of freight transport. As the economic lifeblood of the global economy critical to the United States national interests, the MTS connects America's consumers, producers, manufacturers, and farmers to domestic and global markets.

The MTS also enables critical national security sealift capabilities, supporting U.S. Armed Forces' logistical requirements around the globe. Nationally, 56 of our 361 ports are considered to be strategic due to their importance for the US economy, national security, execution of US Campaign Plans, and sustaining national transportation of goods. Fifty-one of those 56 strategic ports are civilian owned. Twenty-two strategic ports are part of the National Port Readiness Network (NPRN), which assists in overseeing and coordinating readiness for strategic sealift as mandated by the Jones Act and Maritime Security Program. Seventeen of the 22 ports in the NPRN are civilian seaports and six are military seaports. From 2001-2019, over 90 percent of war winning materials flowed through those 22 ports in support of overseas contingency

³⁵ <https://media.defense.gov/2018/Oct/05/2002049100/-1/-1/1/USCG%20MARITIME%20COMMERCE%20STRATEGIC%20OUTLOOK-RELEASABLE.PDF>.

³⁶ <https://www.maritime-executive.com/article/u-s-port-economic-impact-rises-dramatically>.

2020 Maritime Security Plan

operations (OCO). Any significant disruption to the MTS, whether man-made or natural, has the potential to cause cascading and devastating impacts to our domestic and global supply chain and, consequently, America's economy and national security.

Enhancing the security of and protecting U.S. interests in the maritime domain are national security policy objectives administered by DHS, through the USCG, TSA, and CBP. This includes preventing terrorist attacks and strengthening U.S. national and homeland security by protecting the Nation's critical transportation infrastructure, borders, ports, waterways, and coastal approaches in the MTS. Maritime elements of the vital global supply chains serving the Nation are among the critical assets and systems that must be protected. CBP and DHS CWMD 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 domestic trade and security protocols. TSA administers the Transportation Worker Identification Credential (TWIC) program for transportation personnel that need access to secure or restricted areas of port facilities and the USCG enforces TWIC compliance. Federal, state, and local authorities, and industry personnel engage via the USCG's Area Maritime Security Committee (AMSC) at the port level to ensure the safety, security, and resilience of our Nation's critical MTS.

Through effective coordination, collaborative planning, open communications, and strong working relationships, AMSCs have proven their value to bolstering the safety and security of the MTS. There are currently 43 AMSCs across the Nation. The Federal Emergency Management Agency complements these efforts by providing funds through the Port Security Grant Program.

The 2011 Maritime Operations Coordination (MOC) Plan states that a Regional Coordinating Mechanism (ReCoM) will be established for each U.S. Coast Region to coordinate component maritime operational activities. The MOC Plan is a Department of Homeland Security cross-component agreement between U.S. Coast Guard, U.S. Customs and Border Protection and U.S. Immigration and Customs Enforcement for maritime operational coordination, planning, information sharing, intelligence integration, and response activities for an efficient, effective and coordinated Departmental response to threats against the homeland.

4) Risk Profile

Terrorism Risk: A successful terrorist attack in the MTS, 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 the reliance on maritime 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 and preventing suspicious activity in the maritime domain adjacent to and within United States borders.

2020 Maritime Security Plan

Weapons of Mass Destruction (WMDs): 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. Because they are not subject to the same regulations as larger vessels, including not being required to broadcast Automatic Identification System (AIS) locational and identification data, vessels less than 300 gross tons (considered small vessels) could be targeted by terrorists or saboteurs as opportunities to smuggle dangerous weapons, including WMDs, 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 United States waterways. Vessels less than 300 gross tons not engaged in commercial services are also not required to carry electronic identification devices, make advance notices of arrival, or otherwise alert authorities to their whereabouts;³⁷ 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 4-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, passengers, and crew hostage. Incidents with fast attack boats and unmanned explosive boats in the Persian Gulf and Red Sea illustrate additional tactics that threaten the global supply chain and have implications for U.S. MTS security measures.

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 cyberspace is a global domain, predominately existing with-in the maritime information environment consisting of the interdependent network of maritime information technology infrastructure (IT), maritime operational technology (OT) infrastructures, and maritime resident data, including the internet, the electromagnetic spectrum (predominately radio frequency spectrum), and any telecommunications networks (e.g. undersea cables), computers, information and communications systems, and embedded processors and controllers in, on, under, or relating to maritime processes and functions. Cyber-related risks are a growing portion of the vulnerabilities facing the MTS. Vessel and facility operators use computers and cyber-dependent technologies for navigation, communications, engineering, cargo transfer, ballast, safety, environmental control, and many other purposes. Collectively,

³⁷ Operators of small pleasure vessels, arriving in the United States from a foreign port or place, to include any vessel that has visited a hovering vessel or received merchandise outside the territorial sea, are required to report their arrival to CBP immediately.

2020 Maritime Security Plan

these technologies enable the MTS to operate with an impressive record of reliability and at a capacity that drives the U.S. economy and supports national defense, homeland security, and related needs.

Threats and effects in cyberspace can be achieved by activities in the physical domains such as affecting the electromagnetic spectrum (EMS) or the physical infrastructure. Cyber operations (CO) routinely rely on transmission through the EMS and can be significantly affected by congestion (i.e., unintentional interference from commercial and military use), atmospheric conditions, and enemy electronic attack (EA). The relationship between space and cyberspace is unique in that a critical portion of cyberspace bandwidth can only be provided via space operations, which provide a key global connectivity option for CO. For example, INMARSAT is the gateway for all Internet Protocol on ships underway at sea. Additionally, many aspects of cyberspace operations, Information Technology, and Operational Technology (e.g., ICS) rely on precision, navigation, and timing (PNT) methods, through the EMS, provided by satellite GPS.

While these cyber systems create benefits, they also introduce risk. Exploitation, misuse, or failure of cyber systems could cause injury or death, harm the marine environment, or disrupt vital trade activity. Three quarters of our Nation's commerce passes through our ports and waterways, therefore, even a temporary or partial disruption of MTS operations could have serious consequences for the local, regional, national, and global economy.³⁸

Especially Hazardous Cargo Release: Especially hazardous cargos are transported, transferred, and stored in numerous ports and waterways, particularly the U.S. Gulf Coast region and the Western Rivers.³⁹ 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.

Simple Weapons Attacks: The escalation of small weapons attacks over the past decade are stark reminders that we live in a dangerous world. Active shooter incidents or other attacks using simple tactics such as bladed weapons, explosives, and even vehicles could occur at soft targets and crowded places that exist in the maritime domain, e.g., cruise ship and ferry passenger terminals, marine events, etc. Environments that are easily accessible to large numbers of people on a predictable or semi-predicted basis with limited security are soft targets for would be attackers.

³⁸ https://www.bts.gov/archive/publications/transportation_statistics_annual_report/index.

³⁹ "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).

2020 Maritime Security Plan

B. Risk-Based Priorities

Risk Assessment: 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 better informs AMSCs, 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 USCG also collaborates with DHS 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 five to eight-year time horizon. The maritime risk-based priorities are:

Domestic and international port-level risk assessments: Ensure risk assessments include ports implementation of the Maritime Transportation Security Act (MTSA) and International Ship and Port Facility Security (ISPS) code requirements.

Risk-based security planning and operations: Use risk assessment data to reduce terrorism risk and inform the activities in a robust planning, execution, tracking, and reporting process.

International maritime security regime: Assess the implementation of the ISPS code in foreign ports and address non-compliance.

Maritime domain awareness: Understand the broad view of maritime activities and integrate traditional intelligence processes with persistent monitoring of the MTS.

Maritime security and response operations: Collaborative, coordinated, integrated, and layered operations conducted by the USCG and its maritime security partners to deny use and exploitation of the maritime domain by criminal or hostile actors.

Cyber safety, security, and resilience: Promote implementation of the National Institute of Standards and Technology (NIST) cybersecurity framework with public and private maritime infrastructure owners/operators.

2020 Maritime Security Plan

II. Objectives, Activities, and Measuring Progress

The Maritime Security Plan’s goals and objectives reflect the risk-based priorities, and supports national objectives outlined in the National Strategy for Maritime Security.⁴⁰ Figure 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 maritime security.

Figure 8: Maritime Security Goals

NSTS Goal 1	Manage risks to transportation systems from terrorist attack and enhance system resilience
Objective 1.1: Use risk based security planning and operations to reduce the terrorism risk to the Marine Transportation System.	Activity 1.1.1: Improve compliance in MTSA-regulated facilities through risk-based adjustment of enforcement operations tempo. (DHS/USCG) Outcome: Reduce vulnerabilities at high-risk maritime facilities and vessels. Performance Measurement: Security compliance rate for high-risk maritime facilities. (DHS/USCG)
	Activity 1.1.2: Improve interoperability of federal, state, local, territorial, and tribal response teams in Maritime and Security Response Operations (MSRO). (DHS/USCG) Outcome: Reduce risks of terrorist planning and precursor activities. Performance Measurement: Percentage change from year-to-year in port-level deployments of MSRO. (DHS/USCG)
	Activity 1.1.3: 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 at U.S. ports. (DHS/USCG) Outcome: Improve port risk evaluations to reduce port vulnerabilities. Performance Measurement: Percentage change in port risk estimates. (DHS/USCG)
	Activity 1.1.4: 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/CBP)

⁴⁰ <https://www.hsdl.org/?abstract&did=456414>.

2020 Maritime Security Plan

NSTS Goal 1	Manage risks to transportation systems from terrorist attack and enhance system resilience
<p>Objective 1.2:</p> <p>Reduce security vulnerabilities and improve preparedness throughout the Marine Transportation System.</p>	<p>Activity 1.2.1: Assess ISPS Code implementation in foreign ports that receive ships destined for the United States. (DHS/USCG)</p> <p>Outcomes: Assess security (identify risks) at foreign ports serving ships destined for the United States.</p> <p>Performance Measurement: Percentage of trading partners assessed. (DHS/USCG)</p> <hr/> <p>Activity 1.2.2: Evaluate containerized cargo for illicit radiological or nuclear material. (DHS/CBP/CWMD)</p> <p>Outcome: Reduce the risk of illicit radiological or nuclear material entering the United States.</p> <p>Performance Measurement: Percentage of containerized cargo conveyances that pass through radiation portal monitors at sea ports of entry per 6 USC 982b. (DHS/CBP)</p>

2020 Maritime Security Plan

NSTS Goal 2:	Enhance effective domain awareness of MTS and threats
<p>Objective 2.1: Improve the security, resilience, and regulatory (federal, state, local, tribal, and territorial government levels) information sharing process throughout the Marine Transportation System community.</p>	<p>Activity 2.1.1: Enhance resilience of cyber systems through implementation of the National Cyber Strategy Implementation Plan, exercises, guidance, assessments, and expansion of cyber intrusion detection and remediation technology. (DHS/USCG/CISA)</p> <p>Outcome: Improve awareness of and action to reduce the risk of cyber threats or malware.</p> <p>Performance Measurement: Percentage of the Area Maritime Security Plans that have been approved and implemented for cyber-related risks. (DHS/USCG)</p> <p>-----</p> <p>Activity 2.1.2: Participate in and materially support the development of a national Maritime Domain Awareness tool as defined in the Maritime SAFE Act⁴¹ (DHS, TSA, USCG)</p> <p>Outcome: Improve whole-of-government Maritime Domain Awareness and information sharing</p> <p>Performance Measurement: Percentage of USCG, CBP, TSA, State Fusion Centers, Vessel Tracking Systems, and analysis centers with access to the MDA tool. (DHS, TSA, USCG)</p>
<p>Objective 2.2: Improve Marine Transportation System stakeholder participation in the risk management process for security and resilience prioritization and programming.</p>	<p>Activity 2.2.1: Improve effectiveness of port exercise programs by designing exercise objectives and events based on analysis of MSRAM risk data. (DHS/USCG)</p> <p>Outcome: Improve risk-based design of port exercises.</p> <p>Performance Measurement: Percentage of security exercises that include use of MSRAM data. (DHS/USCG)</p>
NSTS Goal 3:	Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce
<p>Objective 3.1: Collaborate with international partners to increase the reliability of the global supply chain.</p>	<p>Activity 3.1.1: Apply risk segmentation methods to evaluate cargo for expeditious clearance. (DHS/CBP)</p> <p>Outcome: Secure and expedite trade.</p> <p>Performance Measurement: Percentage of cargo by value imported to the United States by participants in CBP trade partnership programs. (DHS/CBP)</p>

⁴¹ <https://www.govtrack.us/congress/bills/116/s1269>

2020 Maritime Security Plan

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.

National Security Presidential Directive-41/Homeland Security Presidential Directive (HSPD) 13, “Maritime Security Policy,” directed the development of a National Strategy for Maritime Security (NSMS).⁴² Eight additional supporting plans (later incorporated into the NSMS) were required to address, in greater detail, certain aspects of maritime security including recovery from disruptions.⁴³ 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.⁴⁴ 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, upon successful resolution of security incidents through the Maritime Operational Threat Response (MOTR) Plan managed by the Global MOTR Coordination Center,⁴⁵ the MIRP focuses on restoring maritime transportation capabilities (that is, restoration of passenger and cargo flow), expediting the recovery of trade, and minimizing the impact of a disruption on the U.S. economy.

In addition, the USCG developed MTS Recovery Plans (MTSRP) for each of its Captain of the Port Zones. The MTSRPs support all-hazard recovery and restoration of the MTS’s ability to resume port operations, and the resumption of trade following a disruption. Responsibilities extend to incident and non-incident areas, requiring engagement with a broad spectrum of port stakeholders within the maritime modal and intermodal communities. The MTSRP establishes effective and efficient steps to facilitate measurable short-term recovery of the MTS and support restorative efforts beyond the initial response/recovery phase.

Because no single government agency or private sector organization possesses the responsibility, the resources, or the awareness needed to manage the recovery of the MTS following a maritime incident, this protocol establishes a process for collaborative recovery of maritime trade. The MTS is vulnerable to events or other circumstances that can significantly affect international

⁴² NSPD-41/HSPD-13 was superseded by Presidential Policy Directive-18, Maritime Security, August 2012, updating and reinforcing the directive for the National Strategy for Maritime Security.

⁴³ 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. The National Plan to Achieve Maritime Domain Awareness and the Global Maritime Intelligence Integration Plan were merged into a new National Maritime Domain Awareness Plan in December 2013 with Revision 1 promulgated in 2017.

⁴⁴ https://www.dhs.gov/sites/default/files/publications/HSPD_MIRPPlan_0.pdf. Accessed May 4, 2017.

⁴⁵ <https://www.dhs.gov/global-motr-coordination-center-gmcc>.

2020 Maritime Security Plan

maritime trade. Actual or potential events include all hazards such as natural disasters, Transportation Security Incidents (TSIs), major maritime incidents, declaration of an Incident of National Significance (INS), or other circumstances significantly affecting the MTS.

For the purposes of the "USCG Joint Protocols for the Expeditious Recovery of Trade," recovery is defined as "activities related to recovery of the functionality of the MTS and its capability to handle cargo and passenger traffic" in that period commencing with response to an incident and continuing into the initial phase of restoration of full capability of the MTS. The actual time will vary, but generally starts within three days of the incident and may continue for a period of up to 90 days.

These protocols are intended to specify actions to be taken to recover the functionality of the MTS after an event, or potential event, causing a major disruption of the MTS. The goals of these protocols are to:

- Consider the collateral impacts of a major disruption of the MTS on international commerce.
- Support federal decision-making and the protection of federal interests.
- Establish how the USCG and CBP will interact with other government agencies to jointly facilitate the expeditious recovery of the national MTS and resumption of commerce, including Maritime Infrastructure Recovery Plan (MRP)-related activities.
- Support Presidential Policy Directive-18, Maritime Security
- Support the SAFE Port Act of 2006 mandate to develop protocols for the resumption of trade in the event of a transportation disruption.

Various federal statutory authorities and policies provide the basis for federal actions and activities in a maritime infrastructure recovery. These protocols use the foundation provided by the National Strategy for Maritime Security (now under Presidential Policy Directive-18, Maritime Security in conjunction with the National Maritime Transportation Security Plan (NMTSP) and the Maritime Infrastructure Recovery Plan (MIRP) to provide guidance for the recovery of the MITS and cargo flow.



Appendix C: 2020 Surface Security Plan



**Homeland
Security**

Transportation Security Administration

2020 Surface Security Plan

Surface Transportation Overview

The 2020 Surface Security Plan fulfills a requirement established by 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.⁴⁶ The Surface Security Plan includes the modal plans for mass transit and passenger rail (MTPR), freight rail (FR), highway and motor carrier (HMC), and pipeline as shown in Figure 9.

In addition to fulfilling IRTPA requirements, the Surface Security Plan also fulfills a requirement established by the 9/11 Act to develop and implement a strategic-level framework to manage risks to public transportation and rail transportation systems from terrorist attack or other major incident.⁴⁷ The overarching Surface Security Plan in combination with the MTPR and FR modal plans outline the strategic approach used to secure public and rail transportation through:

- Identification and delineation of roles and responsibilities of appropriate surface transportation stakeholders
- Identification of risk-based priorities that are informed by security assessments and threat analyses
- Identification and application of research and development practices and technologies that can be leveraged to enhance security effectiveness
- Other actions such as the administration of security grant funding

Figure 9: 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. Approximately 6,800 local transit providers serve 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 almost 32 million passengers in FY 2018.
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 86,000 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 their open-access stops and stations, school buses and their open-access stops, and 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 U.S. 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.

⁴⁶ 49 U.S.C. § 114(s).

⁴⁷ 6 U.S.C. § 1133.

2020 Surface Security Plan

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. This includes planning, training, exercises, information sharing, cybersecurity and infrastructure protection, risk-reduction, and community outreach as shown in Figure 10.

These seven risk-based priorities provide the foundation for supporting objectives and activities shown in Figures 11, 12, 13, and 15. 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 risk-based priorities provide the programmatic focus for this plan's activities to reduce terrorism risks identified in each mode's risk profile and risk scenario sections.

Figure 10: Risk-Based Priorities and Objectives

Security Planning	Ensure a planned, documented, organized response to actual and potential security threats to the system, and to address these threats with proactive measures and response techniques that manage and minimize the outcome of security breaches or related events.
Security Training	Ensure surface transportation agencies personnel are trained, tested, and monitored in security awareness, emergency response protocols, and other agency procedures appropriate to their position.
Security Exercises	Ensure surface transportation agencies' engagement in exercises such as table-top, functional, and full-scale exercises in preparation for a terrorist attack, and test the effectiveness of security programs by identifying gaps in their preparedness measures.
Cybersecurity and critical infrastructure protection	Cyber includes information systems, programmable electronic devices, computers or other automated systems that are directly used in providing transportation, and back-up systems. Critical infrastructure includes platforms, stations, intermodal terminals, data and dispatching centers, switching and storage areas, fixed locomotive fueling facilities, classification yards, tunnels, bridges, pipelines, and corporate facilities.
Operational detection and deterrence	Personnel screening, security incident procedures, National Terrorism Advisory System response procedures, training and awareness, physical security and access control measures, etc.
Intelligence and security information sharing	Sharing of transportation security information between the Federal Government and private and public stakeholders. Collaboration between transportation security partners to achieve a common understanding of challenges, impacts, and feasible solutions.
Community outreach	Security awareness outreach efforts to neighbors, law enforcement, media, and the public.

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

2020 Surface Security Plan

needs. The strategy's success relies heavily on the partnerships built and sustained between public and private owners and operators to enhance surface transportation security through deterrence, detection, and resilience activities.

TSA recognizes that sharing of intelligence and information with public transportation owners and operators, continuous analysis and communication of threats to all transportation stakeholders (including the public, as appropriate), establishing 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, are essential to ensuring the safety of movement of people and commodities and the infrastructure vital to their movement.

Roles and Responsibilities

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 DOT (that is, Federal Transit Administration, Federal Railroad Administration, the Pipeline and Hazardous Materials Administration [PHMSA], the Federal Highway Administration, the Federal Motor Carrier Safety Administration, the Federal Bureau of Investigation (FBI), the Federal Energy Regulatory Commission (FERC), and U.S. Department of Energy [DOE]).

Federal Government responsibilities include:

- Assessing intelligence to identify individuals who pose a threat to transportation security
- Sharing threat information and communicating risk mitigation measures 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
- Coordinating across Government Coordinating Councils

State, Local, Tribal, and Territorial Government Entities

State, local, tribal, and territorial government entities are generally the first to respond to terrorist incidents involving surface transportation. Consequently, state, local, tribal, and territorial governments are best positioned to identify and address specific public transportation security needs and to lead local preparedness efforts.

2020 Surface Security Plan

State, local, tribal, and territorial responsibilities include:

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

Industry

Public and private 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, the nature of the security risks, and applicable law.

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 Sector Coordinating Councils, peer advisory groups, and working groups
- Acting on and sharing intelligence reports, security awareness messages, and other federal, state, local, tribal, and territorial government transportation security communication
- Incorporating “best practices” into day-to-day operations

Industry associations represent many owners and operators in collaborative forums with federal and state, local, tribal, and territorial government entities. For example, the Sector Coordinating Council, chartered under the Critical Infrastructure Partnership Advisory Council (CIPAC), enables quick consultation and advice from industry to the government.⁴⁸

Established in July 2019 pursuant to the TSA Modernization Act of 2018 (P.L. 115-254), the Surface Transportation Security Advisory Committee (STSAC), will serve to advise the TSA Administrator on key surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

⁴⁸ <https://www.dhs.gov/transportation-sector-charters-and-membership>.

2020 Surface Security Plan

The STSAC includes voting members representing the surface modes of transportation, as well as, non-voting members from other departments or agencies with oversight of surface transportation.⁴⁹

The STSAC will focus on priorities established by the TSA Administrator; examples of these priorities include cybersecurity, insider threat, and the measurement of the effectiveness of security practices. Much like the Aviation Security Advisory Committee, the STSAC may form subcommittees or working groups to address specific focus areas and propose recommendations to the full committee for consideration.

Standards and Guidelines

TSA works with industry partners to develop non-regulatory standards and guidelines that serve as model practices within or across the surface transportation modes. Known as security action items, best practices, or guidelines, these documents are developed in cooperation with industry operators and trade associations.

To ensure that there is adoption and adherence to established guidelines and standards, TSA conducts assessments to determine the level of adoption and adherence within a mode of transportation. Examples of these assessments include pipeline corporate security reviews and critical facility security reviews, mass transit/passenger baseline assessment for security enhancement (BASE), and highway motor carrier BASE.

Collectively, the development of non-regulatory guidelines and the subsequent assessments of adoption and implementation is known as “Structured Oversight.” TSA uses the structured oversight process to enhance security preparedness and to monitor the security posture of surface transportation operators.

Information Sharing

Evolving and unpredictable security threats to highway-dependent transportation and rail-dependent transportation, as well as pipeline transportation systems, coupled with the expanding environment of infrastructure and carrier systems, call for the continuous sharing of security information and intelligence between government, highway, transit, railroad, and pipeline stakeholders. The NSTS identifies the need for collaboration between transportation security partners to achieve a common understanding of challenges, impacts, and feasible solutions. To achieve these goals, TSA developed the Transportation Security Information Sharing Environment report to “promote sharing of transportation security information between DHS and public and private stakeholders.”⁵⁰ The report describes the process and products available for sharing pertinent threat and incident information, recommended practices, protective measures, and domain awareness updates with stakeholders.

⁴⁹ <https://www.tsa.gov/for-industry/surface-transportation-security>.

⁵⁰ 49 U.S.C. §114(u)3.

2020 Surface Security Plan

Additionally, TSA disseminates Security Awareness Messages (SAM) and Cybersecurity Awareness Messages, providing security information and need for heightened awareness to industry partners and transportation stakeholders. These messages encourage continued vigilance and timely reporting of suspicious incidents and cyber-attacks, reemphasize existing security measures, and recommend voluntary protective measures over designated periods of expected heightened alert such as Memorial Day and Independence Day.

TSA also conducts monthly teleconferences that provide threat updates to law enforcement and security leads for mode-specific transportation. Additionally, it conducts more thorough in-person consultations and coordination with officials from TSA, FBI, DHS, and DOT, which occur three to four times per year. Intelligence and security information is exchanged domestically and internationally on a daily basis through a variety of means implemented by government and industry.

TSA continues to work with its industry and government partners to enhance the development and delivery of intelligence and information products that are timely and relevant. Whether through the auspices of the TSA Field Intelligence Officers or through direct delivery to industry security personnel, there is a continuing need to advance information sharing to meet the challenge of evolving and expanding threats.

Evolving Threats and Technology

UAS, often referred to as drones, are an emerging technology increasingly used for a variety of businesses, research, and recreation purposes. Although most UAS operations are legitimate, they provide opportunities for terrorists to attack surface transportation targets in ways that are difficult to prevent, detect, or deter. The sprawling nature of railroad rights-of-way, highways, pipelines, and rolling stock makes oversight of a UAS threat challenging.

In the surface transportation environment, UAS-related threats may include reconnaissance and surveillance to observe and gather information against a target. Additionally, connecting a poorly secured UAS or UAS control system to a computer network could introduce a vulnerability that a malicious actor could exploit.

Securing surface transportation systems and critical infrastructure from UAS requires collaboration with industry and interagency partners to effectively manage and mitigate risks to their operations, operating environments, passengers, and commodities.

2020 Surface Security Plan

Mass Transit and Passenger Rail Security Strategic Plan

I. Introduction

A. 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. According to the American Public Transportation Association (APTA), 2019 Public Transportation Fact Book, there were over 10 billion public transportation unlinked trips in 2017.⁵¹ Americans board public transportation 34 million times each weekday.⁵² A successful terrorist attack would have a profound impact on ridership and a negative economic impact nationwide. Securing public transportation systems from terrorist attacks is vitally important and a task that demands constant vigilance, innovation, and dedication.

The MTPR Security Strategic Plan provides a strategy that has been collaboratively developed by government officials and industry stakeholders to enhance and sustain capabilities for protection of the Nation's MTPR systems from terrorist attack. This plan meets the modal security planning requirements established by IRTPA and strategic planning requirements of the 9/11 Act.^{53, 54}

The MTPR Security Strategic Plan encourages frequent sharing of intelligence and information with MTPR owners and operators, continuous analysis and communication of threats to all transportation stakeholders (including the public, as appropriate), establishing 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.

1) Modal Profile

The MTPR mode includes public and private transportation agencies and companies. Federal and state, local, tribal, and territorial governments authorize, regulate, and provide financial support—in varying degrees—to many public and private MTPR operations. Reducing security vulnerabilities in transit and passenger rail operations, critical assets, and infrastructure is a collaborative and shared responsibility between TSA and MTPR 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

⁵¹ https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf. Accessed June 10, 2019.

⁵² <https://www.apta.com/news-publications/public-transportation-facts/>.

⁵³ 49 U.S.C. § 114(s).

⁵⁴ 6 U.S.C. § 1133.

2020 Surface Security Plan

information, and facilitating security drills and exercises. TSA also provides operational support in the form of providing trained explosives detection canines to MTPR systems, conducting First Observer Plus™ training to frontline workers and supporting random baggage screening. While security initiatives outlined in this strategic plan extend to all MTPR operators, this plan focuses on those agencies that are identified as higher-risk—transit agencies that service the regions with the highest transit-specific risk. Risk ranking is based on considerations related to ridership, location of services provided (use of the same stations and stops), and relationship between feeder and primary systems.

Passenger rail is divided into two categories: inter-city 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. They sometimes control, operate, and maintain tracks, facilities, construction sites, utilities, and computerized networks essential to their own operations.

The sole long-distance inter-city passenger railroad in the contiguous United States is Amtrak, which has an annual ridership of approximately 31.7 million.⁵⁵ Amtrak operates a nationwide rail network, serving more than 500 destinations in 46 states, the District of Columbia, and three Canadian provinces on more than 21,300 track-miles.⁵⁶ Freight railroads own and control 72 percent of the track on which Amtrak operates.⁵⁷ A notable exception is the North East Corridor, an electrified railway line in the Northeast megalopolis of the United States owned primarily by Amtrak. It runs from Boston through New York City, Philadelphia, Baltimore, and terminus in Washington, D.C. In fiscal year 2018, the Northeast Corridor saw a ridership of 12.12 million.⁵⁸

Rail passenger transportation services are provided by 25 commuter railroads operating in several metropolitan areas. Dozens of the commuter railroads operate or plan to operate at least partially on freight-owned corridors. Additionally, most of the higher speed and inter-city passenger rail projects under development plan to use freight-owned tracks and infrastructure.

TSA and its government partners like FEMA strive to advance MTPR 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 FEMA, and other resources to address risks. TSA also works closely with MTPR systems to identify and assess vulnerabilities of the higher-risk MTPR systems both for operational activities and critical infrastructure assets of national importance. TSA works with agencies to identify resources, including grants, and to implement programs that buy-down risk and mitigate identified vulnerabilities.

⁵⁵https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf. Accessed June 10, 2019.

⁵⁶https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf. Accessed June 10, 2019.

⁵⁷<https://www.amtrak.com/national-facts>. Accessed May 11, 2017.

⁵⁸ https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf. Accessed June 10, 2019.

2020 Surface Security Plan

2) Risk Profile

Public transportation systems face significant challenges in making their systems secure. Certain characteristics make them both vulnerable and difficult to protect. 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—such as the presence of visible law enforcement, the use of explosives detection canines, random passenger bag inspections, and counter-surveillance activities—help 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 offenders or terrorist teams. Elevated risks are also associated with bridges, and underground and underwater tunnels, common to many MTPR routes.

While few terrorist attacks or attempted attacks have occurred against MTPR assets in the United States since 9/11, public transportation systems are common targets overseas. Most overseas attacks targeted buses, railroad tracks, mass transit trains, and bus stations, and have ranged from complex attacks using VBIEDs or suicide attackers to attacks by lone offenders using edged weapons. Terrorist tactics and techniques used overseas could easily be used to conduct similar attacks in the United States.

3) Risk Scenarios and Security Assessments

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.

Primary risk scenarios for public transportation include:

- Armed assault and active-shooter situations
- Chemical/biological attacks
- Cyber-attack
- IEDs (person borne/suicide) aboard a train/in a station/on a platform
- Insider threat (defined by the DHS Insider Threat Program as “the threat that an employee or a contractor will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States”)⁵⁹
- Sabotage of infrastructure causing derailment
- Vehicle ramming

⁵⁹ www.dhs.gov/science-and-technology/cybersecurity-insider-threat.

2020 Surface Security Plan

Operationally, the risk scenarios inform the selection of activities used to implement risk-based priorities and address security vulnerabilities.⁶⁰ Along with physical threats, cyber threats that could disrupt operations or affect safe operation of transit systems remains a concern.

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 (TSSRA). 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 security-related incidents.

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.

The new TSSRA version (now in pre-release review) adds the risk scenario—vehicle ramming attack on pedestrian concentrations in areas with adjacent, open-access roadways.

B. Threat Analysis

TSA issues modal threat assessments semi-annually as well as specific and recurring analyses of incidents that provide context on the terrorism threat to the United States, the Transportation Sector, and passenger railroads. These products describe key terrorist actors and group ideologies, recent attacks, modes of attack, and other tactics, techniques, and procedures used by HVE and provide a threat level based on these analyses. Operationally, these assessments help federal, state, and local government security officials and industry professionals protect mass transit systems and passenger railroads from attacks.

⁶⁰ Transportation Sector Security Risk Assessment 5.0 (2016).

2020 Surface Security Plan

C. Research and Development

Transportation security and resilience are enhanced through the identification and application of existing, emerging technologies, and processes that address capability gaps. Technology enhancements improve effectiveness of security and resilience, lead to operational efficiencies, and often reduce costs. Both government and the transportation industry participate in 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 (DHS S&T, TSA, and DOT).

D. Other Actions

Transit Security Grant Program

Security Grant Programs, including the Transit Security Grant Program, Intercity Passenger Rail Security Grant Program (Amtrak), and the Intercity Bus Security Grant Program, authorized by 9/11 Act sections 1406, 1513, and 1536 respectively, are administered by FEMA in collaboration with TSA. They directly support public transportation operational and capital infrastructure security activities.

Security grant funds are appropriated annually and awarded to eligible applicants (which include intra-city bus, commuter bus, ferries, and all forms of passenger rail). They support the creation of sustainable, risk-based efforts to protect critical infrastructure and the traveling public from acts of terrorism, major disasters, and other emergencies.

Security Regulations

Part 1580 of title 49 of the Code of Federal Regulations establishes rules for the security of passenger rail transportation. The rules apply to each operator of a rail transit system including passenger rail and commuter rail, 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.

Part 239 of title 49 requires passenger railroads in commuter or inter-city service to have emergency preparedness plans, provide training to employees, and conduct exercises with emergency responders to test and validate their emergency procedures.

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,

2020 Surface Security Plan

and events. Additionally, the 9/11 Act requires public transportation agencies, determined by the Secretary of Homeland Security to be of high-risk for terrorism, to conduct vulnerability assessments and develop comprehensive security plans. TSA is developing regulations to implement these mandates.⁶¹

II. Objectives, Activities, and Measuring Progress

The MTPR goals and objectives reflect the risk-based priorities. Figure 11 highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass a government-wide approach to national MTPR security. 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 are needed in refining outcomes, developing methodologies, and collecting data.

Figure 11: Mass Transit and Passenger Rail Security Goals

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
<p>Objective 1.1 Security Planning:</p> <p>Reduce the risks associated with a terrorist attack on MTPR systems through security plans that address cybersecurity and critical infrastructure protection, and operational practices (to detect and deter).</p>	<p>Activity 1.1.1: Develop, review, and update security plans based on available information. (Industry/DHS/TSA)</p> <p>Outcome: Improvement of industry security plans and security planning for both physical and cybersecurity through incorporation of best practices and lessons learned.</p> <p>Performance Measurement: Percentage of high-risk transit agencies assessed during the measurement period that achieved a positive rating for security planning using the BASE. (DHS/TSA)</p> <hr/> <p>Activity 1.1.2: Develop a comprehensive cybersecurity strategy. (Industry/DHS/TSA)</p> <p>Outcome: Improvement of industry security awareness and preparedness to identify and protect against cybersecurity threats to the system.</p> <p>Performance Measurement: Percentage of high-risk transit agencies assessed during the measurement period that achieved a positive rating for security planning using the BASE. (DHS/TSA)</p>
<p>Objective 1.2 Security Training:</p> <p>Conduct training of employees to identify, prevent, respond, and recover from a terrorist attack.</p>	<p>Activity 1.2.1: 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)</p>

⁶¹ As required by sections 1408, 1512, and 1517 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. 110-53 (August 3, 2007).

2020 Surface Security Plan

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
	<p>Outcome: Improve capability of industry employees to identify, prevent, respond to, and recover from a physical or cyber terrorist attack.</p> <p>Performance Measurement: Percentage of high-risk transit agencies assessed during the measurement period that achieved a positive rating for security training using the BASE assessment. (DHS/TSA)</p>
<p>Objective 1.3 Security Exercises:</p> <p>Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.</p>	<p>Activity 1.3.1: MTPR systems participate in exercises to evaluate the preparedness for, response to, and recovery from physical and cybersecurity incidents. (Industry/DHS/TSA)</p> <p>Outcome: MTPR systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents.</p> <p>Performance Measurement: Percentage of high-risk transit agencies assessed during the measurement period that achieved a positive rating for security exercises, including TSA's Intermodal Security Training Program exercises, using the BASE. (DHS/TSA)</p>
NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
<p>Objective 2.1 Intelligence and Information Sharing:</p> <p>Maintain and enhance mechanisms for information and intelligence sharing between the MTPR industry and government.</p>	<p>Activity 2.1.1: Provide timely and relevant information and intelligence to enhance industry's domain awareness. (DHS/TSA)</p> <p>Outcome: Sustain domain awareness through timely delivery of relevant intelligence and information products for MTPR industry to implement mitigation strategies to reduce risk.</p> <p>Performance Measurement: Percentage of intelligence products delivered to MTPR stakeholders within 24 hours of release. (DHS/TSA)</p>
<p>Objective 2.2 Community Outreach:</p> <p>Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with MTPR systems.</p>	<p>Activity 2.2.1: Promote MTPR security awareness in communities surrounding critical MTPR assets and systems. (DHS/TSA)</p> <p>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.</p> <p>Performance Measurement: Percentage of high-risk transit agencies assessed during the measurement period that achieved a positive rating for public awareness and emergency preparedness programs using the BASE. (DHS/TSA)</p>

2020 Surface Security Plan

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 state, local, and federal governments 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 DOT's disaster recovery website.⁶² The guidance encourages transit service operators to plan 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.⁶³ 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. However, fundamental principles provided on DOT's disaster recovery website and their emergency preparedness, response, and recovery information website should be applied in transit system planning and exercise.^{64,65} Effective coordination and integration of all entities contributing to disaster response and recovery are necessary for quick recovery of essential public transportation services.

⁶² <https://www.transportation.gov/disaster-recovery>.

⁶³ Information on the frameworks is provided on the FEMA website: <https://www.fema.gov/national-planning-frameworks>.

⁶⁴ <https://www.transportation.gov/tags/disaster-recovery>.

⁶⁵ <https://www.transportation.gov/emergency>.

2020 Surface Security Plan

Freight Rail Security Strategic Plan

I. Introduction

A. Overview

The Freight Rail Security Strategic Plan provides a strategy that 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 and the strategic planning requirements of the 9/11 Act.^{66,67}

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.

The Freight Rail Security Strategic Plan encourages the following activities:

- 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
- Establishment of risk-based priorities to ensure appropriate resourcing and administration of security measures
- Assessment of risks to freight and passenger railroad transportation systems through on-site security assessments and reviews

1) Modal Profile

The national freight rail network is a complex system that includes both physical and cyber infrastructure and consists of approximately 138,000 rail miles operated by seven Class I railroads—railroads with operating revenues of \$463.8 million or more, 21 regional railroads, and 580 local (also known as Short Line) railroads. The Class I railroads account for approximately 60 percent of freight rail mileage, 88 percent of employees, and 94 percent of revenue. Regional railroads and local railroads range in size from operations handling a few carloads monthly to multi-state operators nearly the size of a Class I operation.⁶⁸

⁶⁶ 49 U.S.C. § 114(s).

⁶⁷ 6 U.S.C. § 1161.

⁶⁸ <https://www.aar.org/wp-content/uploads/2018/08/Overview-of-Americas-Freight-RRs.pdf>.

2020 Surface Security Plan

Freight railroads are private entities which own and are responsible for their own infrastructure. They maintain the locomotives, rolling stock, and fixed assets involved in the transportation of goods and materials across the Nation's rail system. As required by Congress, railroads are subject to safety regulations put forth and enforced by the Federal Railroad Administration (FRA). TSA administers and enforces rail security regulations contained in 49 CFR Part 1580. 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 2020 Freight Rail Security Plan focuses on railroad assets and operational areas with the greatest risk of potential attack and thus the 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 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 track are exposed to additional risk of attacks directed at passenger trains or stations. 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.

2020 Surface Security Plan

3) Risk Scenarios and Security Assessments

Freight rail attack scenarios focus on attacks causing mass casualties or disruption of the rail network. They inform the selection of activities to implement the risk-based priorities and countermeasures to address security vulnerabilities.^{69,70}

- 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 damage to critical infrastructure, with potential for ensuing critical impacts on U.S. supply chain security
- Simple attacks using small arms or IEDs
- Insider threat

Risk assessments consider various threat scenarios and the vulnerabilities and consequences attributed to them. TSA's primary risk assessment tool is the TSSRA. The process used to perform the assessment elicits detailed analyses of the vulnerabilities to and consequences of an attack on a transportation target. The results of the assessments are used to compare risks across the modes, inform risk-based priorities, and recommend 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.

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. In context, 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 RSSM.

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.

⁶⁹ Transportation Sector Security Risk Assessment 5.0 (2016).

⁷⁰ 2016 Freight Rail Modal Threat Assessment (TSA Office of Intelligence and Analysis).

2020 Surface Security Plan

B. Threat Analysis

TSA issues modal threat assessments semi-annually as well as specific and recurring analyses of incidents that provide context on the terrorism threat to the United States, the Transportation Sector, and freight railroads. These assessments provide a threat level based on key terrorist actors and group ideologies, recent attacks, modes of attack, and other tactics, techniques, and procedures. Operationally, these assessments help federal, state, and local government security officials and industry professionals protect U.S. railroads from attacks.

C. 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 improve effectiveness of security and resilience, 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 (such as, DHS Science and Technology, TSA, and DOT).

D. Other Actions

Security Regulations

Part 1580 of title 49 Code of Federal Regulations establishes rules for the security of rail transportation. The rules apply to railroad carriers that are part of the general railroad service system of transportation. The regulations require each carrier to appoint a security coordinator, report significant security concerns to TSA, and for freight railroads to implement procedures for the secure custody and transfer of RSSM.

The Hazardous Materials Regulations (title 49 Code of Federal Regulations, Parts 100-180), which are issued by DOT Pipeline and Hazardous Materials Safety Administration (PHMSA), also include provisions for the security of hazardous materials in transportation. These regulations require hazardous materials carriers to have security plans and provide security awareness training for employees. Rail carriers must also analyze the routes used for the transportation of explosives, poison inhalation hazard materials, radioactive materials, and high hazard flammable trains to determine the safest and most secure routes.

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, it requires railroads determined by the Secretary of Homeland Security to be of high risk for terrorism to conduct vulnerability assessments and develop comprehensive security plans. TSA is developing regulations to implement these mandates.

2020 Surface Security Plan

II. Objectives, Activities, and Measuring Progress

The 2020 Freight Rail Security Plan's goals and objectives reflect the risk-based priorities. Figure 12 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. 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.

Figure 12: Freight Rail Security Goals

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
<p>Objective 1.1 Security Planning:</p> <p>Reduce the risks associated with terrorist attacks on freight railroads through security plans that address cybersecurity and critical infrastructure protection, and operational practices (to detect and deter.</p>	<p>Activity 1.1.1: Develop, review, and update security plans based on available information. (Industry/DHS/TSA)</p> <p>Outcome: Improvement of railroad security plans and security planning through incorporation of best practices and lessons learned into existing security plans.</p> <p>Performance Measurement: Percentage of railroads that transport RSSM in HTUAs with implemented security plans. (DHS/TSA)</p> <hr/> <p>Activity 1.1.2: Develop a comprehensive cybersecurity strategy. (Industry/DHS/TSA)</p> <p>Outcome: Improvement of railroad cybersecurity strategies through incorporation of best practices and lessons learned into existing cybersecurity strategies.</p> <p>Performance Measurement: Percentage of railroads that transport RSSM in HTUAs with implemented cybersecurity strategy. (DHS/CISA/TSA)</p> <hr/>
<p>Objective 1.2 Security Training:</p> <p>Conduct training of frontline employees to identify, prevent, and respond to a terrorist attack.</p>	<p>Activity 1.2.1: Improve freight railroad security training programs through the incorporation of best practices and lessons learned into existing training curriculum. (Industry/DHS/TSA)</p> <p>Outcome: Improved capability of the freight railroad employees to identify, prevent, and respond to a physical or cyber terrorist attack.</p> <p>Performance Measurement: Percentage of frontline employees for railroads that transport RSSM in HTUAs that receive security-related training during the reporting period. (DHS/TSA)</p>

2020 Surface Security Plan

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
<p>Objective 1.3 Security Exercises:</p> <p>Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.</p>	<p>Activity 1.3.1: Railroads participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents. (Industry/DOT/DHS/TSA)</p> <p>Outcome: Railroads and public safety agencies are better prepared to respond and recover effectively in the event of physical and cybersecurity incidents.</p> <p>Performance Measurement: Percentage of railroads that transport RSSM in HTUAs that conducted or participated in security-related exercises. (DHS/TSA)</p>
NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
<p>Objective 2.1 Intelligence and Information Sharing:</p> <p>Maintain and enhance mechanisms for information and intelligence sharing between the freight rail industry and government.</p>	<p>Activity 2.1.1: Provide timely and relevant information and intelligence to enhance freight railroads' domain awareness. (DHS/TSA)</p> <p>Outcome: Sustain domain awareness through timely delivery of relevant intelligence and information products to enable freight rail carriers to implement mitigation strategies to reduce risk.</p> <p>Performance Measurement: Percentage of intelligence products delivered to freight rail stakeholders within 24 hours of release. (DHS/TSA)</p>
<p>Objective 2.2 Community Outreach:</p> <p>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.</p>	<p>Activity 2.2.1: Promote freight railroad security awareness in communities surrounding critical freight assets and systems. (DHS/TSA)</p> <p>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.</p> <p>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. (DHS/TSA)</p>

2020 Surface Security Plan

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 to 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*.^{71,72,73} 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.^{74,75}

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.

⁷¹ <https://www.transportation.gov/disaster-recovery>. Accessed May 30, 2019.

⁷² <https://www.transportation.gov/policy-initiatives/disaster-recovery/recovering-disasters-national-transportation-recovery-strategy>. Accessed October 9, 2019.

⁷³ <https://www.transportation.gov/emergency/usdot-recovery-resource-guide>. Accessed October 9, 2019.

⁷⁴ <https://www.fema.gov/national-preparedness-system>. Accessed May 30, 2019.

⁷⁵ <https://www.fema.gov/national-planning-frameworks>. Accessed May 30, 2019.

2020 Surface Security Plan

Highway and Motor Carrier Security Plan

I. Introduction

A. Overview

The HMC Security Plan establishes risk-based priorities to protect the Nation's roads, bridges, tunnels, cargo carriers, and over-the-road bus 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.⁷⁶

1) Modal Profile

The highway system—comprising commercial trucking, highway transportation infrastructure, over-the-road bus, and school bus operations—is an integral part of the Nation's economy and way of life. In 2017, 575.6 million passenger trips occurred on over-the-road bus and motor coaches, and more than 25 million schoolchildren rode more than 480,000 school buses each day.^{77,78} 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. Bridges, causeways, and underground and underwater tunnels are important infrastructure connections in highway systems requiring special security considerations. While the Nation's highways are resilient, large-scale disruptions of these systems may adversely affect

⁷⁶ 49 U.S.C. § 114(s).

⁷⁷ American Bus Association Foundation's Annual Motor Coach Census (2017) (https://www.buses.org/assets/images/uploads/pdf/FINAL_2017_Census_1.pdf). Accessed October 9, 2019.

⁷⁸ American School Bus Council (<http://www.americanschoolbuscouncil.org/about/>).

2020 Surface Security Plan

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. They have used large vehicles to carry out ramming attacks against pedestrian concentrations at street side bus stops and stations, as well as public spaces such as outdoor markets or holiday-related gatherings. Highway infrastructure is potentially vulnerable to disruption by terrorists with cascading consequences for supply chains and other sectors.

3) Risk Scenarios

The HMC attack scenarios inform the development of risk-based priority planning.^{79,80} These attack scenarios include:

- Attacks using IED or 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
- Intentional contamination of food products during bulk transportation

Since the terrorist attacks of July 2016 in Nice, France, the use of vehicles to ram unprotected crowds with deadly results has grown significantly. TSA and its sister DHS agencies, in cooperation with the FBI and other law enforcement agencies and stakeholders, have created and distributed written preventative recommendations. These initiatives are expected to be featured more prominently in future iterations of the NSTS.

⁷⁹ Transportation Sector Security Risk Assessment 5.0 (2016).

⁸⁰ 2018 Highway and Motor Carrier Modal Threat Assessment (TSA Office of Intelligence and Analysis).

2020 Surface Security Plan

II. Objectives, Activities, and Measuring Progress

The HMC Security Plan's goals and objectives reflect the risk-based priorities. Figure 13 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.

Figure 13: Highway and Motor Carrier Security Goals

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
<p>Objective 1.1 Security Planning:</p> <p>Reduce the risks from a terrorist attack on HMC systems through security plans that address cybersecurity and critical infrastructure protection, and operational practices (to detect and deter).</p>	<p>Activity 1.1.1: Develop, review, and update security plans based on available information. (Industry/DHS/TSA)</p> <p>Outcome: Improvement of industry security plans and security planning through incorporation of best practices and lessons learned into existing security plans.</p> <p>Performance Measurement: Percentage of motor carriers assessed during the measurement period that achieved a positive rating for security planning using the BASE. (DHS/TSA)</p> <hr/> <p>Activity 1.1.2: Develop a comprehensive cybersecurity strategy. (Industry/DHS/CISA/TSA)</p> <p>Outcome: Improvement of industry security awareness and preparedness to identify and protect against cybersecurity threats to the system.</p> <p>Performance Measurement: Percentage of motor carriers assessed during the measurement period that achieved a positive rating for internal and external cybersecurity practices using the BASE. (DHS/CISA/TSA)</p>
<p>Objective 1.2 Security Training:</p> <p>Conduct training of employees to identify, prevent, respond to and recover from a terrorist attack.</p>	<p>Activity 1.2.1: Improve the current state of the most critical motor carriers' security training programs through the incorporation of best practices and lessons learned into existing training plans. (Industry/DHS/TSA)</p> <p>Outcome: Improved capability of the industry employees to identify, prevent, respond to, and recover from a terrorist attack.</p> <p>Performance Measurement: Percentage of motor carriers assessed during the measurement period that achieved a positive rating for security training using the BASE. (DHS/TSA)</p>
<p>Objective 1.3 Security Exercises:</p> <p>Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.</p>	<p>Activity 1.3.1: Motor carriers participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents. (Industry/DHS/TSA)</p> <p>Outcome: Motor carriers and public safety agencies are better prepared to respond and recover effectively in the event of security incidents.</p> <p>Performance Measurement: Percentage of motor carriers assessed during the measurement period that achieved a positive rating for security exercises using the BASE. (DHS/TSA)</p>

2020 Surface Security Plan

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
<p>Objective 2.1 Intelligence and Information Sharing:</p> <p>Maintain and enhance mechanisms for information and intelligence sharing between the HMC industry and government.</p>	<p>Activity 2.1.1: Provide timely and relevant information and intelligence to enhance industry's domain awareness. (DHS/TSA)</p> <p>Outcome: Sustain domain awareness through timely delivery of relevant intelligence and information products for HMC industry to implement mitigation strategies to reduce risk.</p> <p>Performance Measurement: Percentage of intelligence products delivered to HMC stakeholders within 24 hours of release by originating office. (DHS/TSA)</p>
<p>Objective 2.2 Community Outreach:</p> <p>Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with HMC systems.</p>	<p>Activity 2.2.1: Promote HMC security awareness in communities surrounding critical HMC assets. (DHS/TSA)</p> <p>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.</p> <p>Performance Measurement: Percentage of motor carriers assessed during the measurement period that achieved a positive rating for sharing security related information or best practices using the BASE. (DHS/TSA)</p>

2020 Surface Security Plan

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 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*.^{81,82,83} 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.^{84,85}

Most response and recovery actions begin and are managed locally, 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.

⁸¹ <https://www.transportation.gov/disaster-recovery>. Accessed May 30, 2019.

⁸² <https://www.transportation.gov/emergency/usdot-recovery-resource-guide>. Accessed October 9, 2019.

⁸³ [https://www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE FINAL%20Version 08-27-2014.pdf](https://www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE%20FINAL%20Version%2008-27-2014.pdf). Accessed May 30, 2019.

⁸⁴ <https://www.fema.gov/national-preparedness-system>. Accessed May 30, 2019.

⁸⁵ <https://www.fema.gov/national-planning-frameworks>. Accessed May 30, 2019.

2020 Surface Security Plan

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.

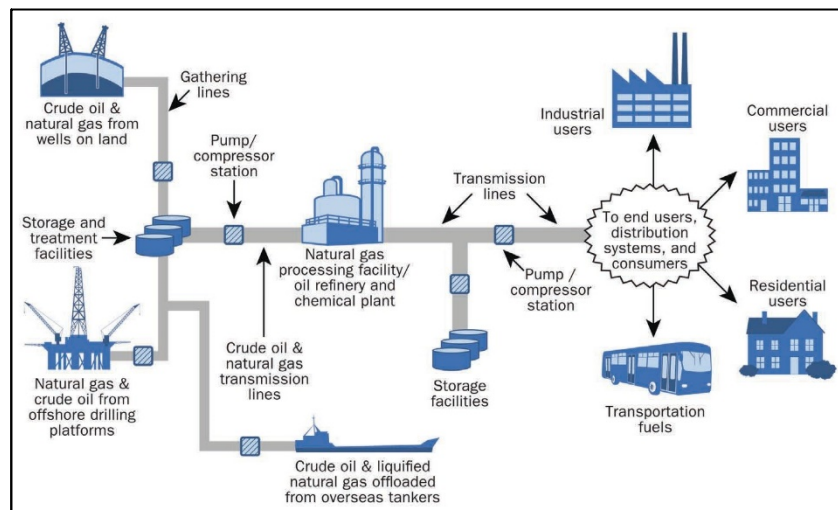
1) Modal Profile

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

Although most pipeline infrastructure is buried underground, operational elements such as compressors, metering, regulating, pumping stations, aerial crossings, and storage tanks are typically located above ground. Under operating pressure, the pipeline systems are used as a conveyance to deliver resources from source location to destination. They are monitored and moderated through automated industrial control systems or SCADA systems. These systems use remote sensors, signals, and preprogrammed 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 (see Figure 14). 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 14: The Structure of Oil and Gas Pipeline Systems Movement to Market



2020 Surface Security Plan

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. Pipeline systems may also be vulnerable to a cyber-attack due to their reliance on operational technology systems. These systems include SCADA systems, process control systems, distributed control systems, measurement systems, and telemetry systems.

From a design-perspective, some pipeline assets are more attractive to terrorists simply because of the transported commodity and the impact an attack would have on national security and commerce. 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 depend on pipeline system commodities.

3) Risk Scenarios

The following risk scenarios inform the selection of activities to implement the risk-based priorities and address security vulnerabilities.^{86, 87, 88}

- Environmental rights extremist or lone offender criminal activity including sabotage, small arms, and vandalism
- HVE explosive attack (IED or VBIED) on an exposed pipeline
- An explosive attack (IED or VBIED) on an exposed toxic inhalation hazard pipeline on a right of way
- Insider threat in which an employee in a control/operations center gains access to systems to shut down or impair service or operations
- Cyber-attack on pipeline operational technology system

⁸⁶ (U/SSI) TSSRA 6.0 (2017) TSSRA 5.0 (2016).

⁸⁷ (U/SSI) TSA Pipeline Annual Terrorism Threat Assessment – 2018.

⁸⁸ (U/SSI) TSA Cyber Modal Threat Assessment – 2017.

2020 Surface Security Plan

II. Objectives, Activities, and Measuring Progress

The Pipeline Security Plan's goals and objectives reflect the risk-based priorities. Figure 15 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.

Figure 15: Pipeline Security Goals

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
<p>Objective 1.1 Security Planning:</p> <p>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.</p>	<p>Activity 1.1.1: Review, implement, and update security plans based on risk and guidance in the TSA Pipeline Security Guidelines. (Industry/DHS/TSA)</p> <p>Outcome: Comprehensive and up-to-date security plans that reduce risk by explicitly addressing pipeline physical security policies and procedures.</p> <p>Performance Measurement: Percentage of pipeline companies whose security plans meet the elements in the TSA Pipeline Security Guidelines as assessed through Corporate Security Reviews (CSRs).⁸⁹ (DHS/TSA)</p> <hr/> <p>Activity 1.1.2: Review, implement, and update cybersecurity plans based on risk and guidance in the TSA Pipeline Security Guidelines. (Industry/DHS/CISA/TSA)</p> <p>Outcome: Comprehensive and up-to-date cybersecurity plans that reduce risk by explicitly addressing pipeline cybersecurity policies and procedures.</p> <p>Performance Measurement: Percentage of pipeline companies whose cybersecurity plans meet the elements in the TSA Pipeline Security Guidelines as assessed through CSRs. (DHS/CISA/TSA)</p>
<p>Objective 1.2 Security Training:</p> <p>Conduct training of employees to identify, prevent, absorb, respond to, and recover from a terrorist attack.</p>	<p>Activity 1.2.1: Review and implement security training programs based on training requirements and guidance in the TSA Pipeline Security Guidelines. (Industry/DHS/TSA)</p> <p>Outcome: Security training that improves the capability of pipeline employees to identify, prevent, absorb, respond to, and recover from a physical or cyber terrorist attack.</p> <p>Performance Measurement: Percentage of pipeline companies whose security training plans and requirements meet the elements in the TSA Pipeline Security Guidelines as assessed through CSRs. (DHS/TSA)</p>

⁸⁹https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf. Accessed May 24, 2019.

2020 Surface Security Plan

NSTS Goal 1	Manage risks to transportation systems from terrorist attacks and enhance system resilience
<p>Objective 1.3 Security Exercises:</p> <p>Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.</p>	<p>Activity 1.3.1: Pipeline systems participate in exercises to evaluate the preparedness for, response to, and recovery from physical or cybersecurity incidents. (Industry/DHS/TSA)</p> <p>Outcome: Pipeline systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents.</p> <p>Performance Measurement: Percentage of pipeline companies whose security drills and exercises meet the elements in the TSA Pipeline Security Guidelines as assessed through CSRs. (DHS/TSA)</p>
<p>Objective 1.4 Physical Security Measures</p> <p>Reduce the risks from an attack on pipeline systems through physical security measures addressing critical infrastructure protection</p>	<p>Activity 1.4.1: Review, implement, and update physical security measures based on risk and guidance in the TSA Pipeline Security Guidelines. (Industry/DHS/TSA)</p> <p>Outcome: Comprehensive and up-to-date physical security measures that reduce risk by addressing site-specific security measures, assessments, barriers, and incident response.</p> <p>Performance Measure: Percentage of pipeline facilities whose physical security and access control measures meet the elements in the TSA Pipeline Security Guidelines as assessed through Critical Facility Security Reviews. (DHS/TSA)</p>
<p>Objective 1.5 Cybersecurity:</p> <p>Reduce the risks from a cyber-attack on pipeline systems through security measures addressing critical infrastructure protection.</p>	<p>Activity 1.5.1: Review, implement, and update cybersecurity measures based on risk and guidance in the TSA Pipeline Security Guidelines. (Industry/DHS/CISA/TSA)</p> <p>Outcome: Comprehensive and up-to-date cybersecurity measures that reduce risk by incorporating National Institute of Standards and Technology Cyber Framework elements.</p> <p>Performance Measurement: Percentage of pipeline companies whose cybersecurity programs meet the elements in the TSA Pipeline Security Guidelines as assessed through CSRs. (DHS/TSA)</p>

2020 Surface Security Plan

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
<p>Objective 2.1 Intelligence and Information Sharing:</p> <p>Maintain and enhance mechanisms for information and intelligence sharing between the pipeline industry and government.</p>	<p>Activity 2.1.1: Provide timely and relevant information and intelligence to enhance industry's domain awareness. (DHS/TSA)</p> <p>Outcome: Sustained domain awareness by pipeline owners and operators through the timely delivery of relevant intelligence and information products allowing them to implement mitigation strategies to reduce risk, as required.</p> <p>Performance Measurement: Percentage of intelligence products delivered to Pipeline stakeholders within 24 hours of release. (DHS/TSA)</p>
<p>Objective 2.2 Community Outreach:</p> <p>Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with pipeline systems.</p>	<p>Activity 2.2.1: Promote pipeline security awareness in communities surrounding critical pipeline assets and systems. (Industry/DHS/TSA)</p> <p>Outcome: Pipeline industry, first responders, and neighboring communities working collectively to enhance security and plan and prepare for incidents that could disrupt pipeline operations and endanger the community.</p> <p>Performance Measurement: Percentage of pipeline companies whose community outreach events meet the elements in the TSA Pipeline Security Guidelines as assessed through CSRs. (DHS/TSA)</p>

2020 Surface Security Plan

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 required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*.⁹⁰ TSA and DOT's PHMSA, 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 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. It 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.

⁹⁰ https://www.tsa.gov/sites/default/files/pipeline_sec_incident_recvr_protocol_plan.pdf. Accessed May 24, 2019.



Appendix D: 2020 Intermodal Transportation Security Plan



**Homeland
Security**

Transportation Security Administration

2020 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 a plan for addressing the security needs of intermodal transportation.”⁹¹ 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.”⁹² 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, this plan focuses on the intermodal movement of supplies, products, mail, and parcels in supply chains.

The transfer of intermodal shipments between modes usually occurs at integrated intermodal terminals as illustrated in Figure 16. These intermodal operations are an integral part of the global supply chain 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 to protect the welfare and interests of the American people and to secure the Nation’s economic prosperity.

As global supply chains become more complex and global in scope, they are increasingly at risk to disruptions stemming from financial, market, natural hazard, accidental, man-made, lack of centralized oversight, and malicious incidents. In some instances, these disruptions could result in large-scale death, destruction, or crippling of the U.S. economy. Therefore, government and private sector stakeholders must ensure operational recovery plans and protocols are in place to restore transportation services following a disruption as quickly as possible.⁹³

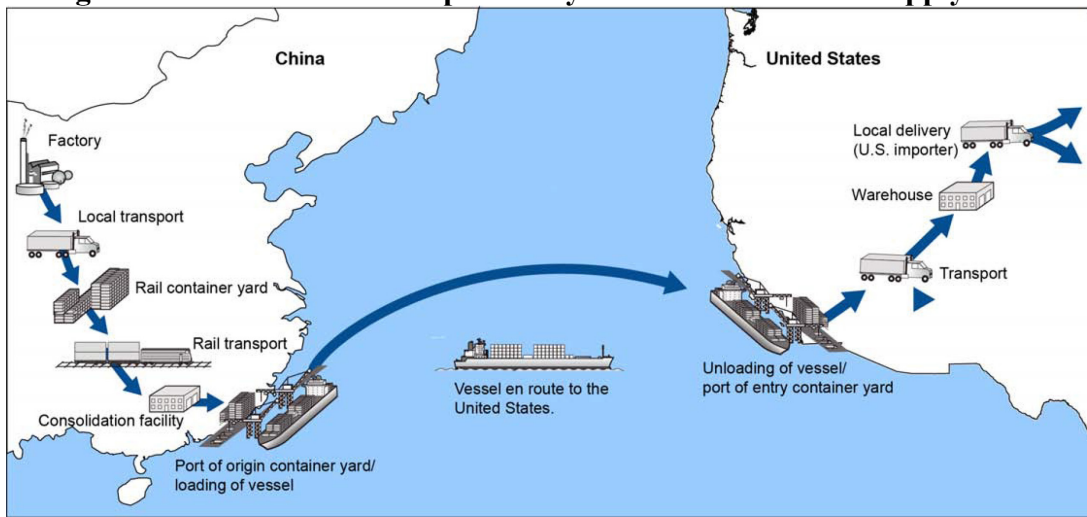
⁹¹ 49 U.S.C. § 114(s)(3)(H).

⁹² Intermodal Surface Transportation Efficiency Act of 1991, Pub. L. No. 102-240, (Dec. 18, 1991).

⁹³ 49 U.S.C. § 114(s)(3)(I).

2020 Intermodal Transportation Security Plan

Figure 16: Illustrative Example of Key Points in the Global Supply Chain



1) Global Supply Chain Profile

The collective modes of trucking, rail, aviation and maritime transportation are just one of the components that support the global supply chain system. The 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 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.

Goods transported through supply chains are handled or managed by many entities from origin to destination, such as shippers, freight forwarders, packers, and unpackers. These entities 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, access control verification, and movement through the various stages of transport. Global supply chain operations are driven by the dynamic, complex nature of international logistics, and operate under a wide variety of international and national rules, regulations, and protocols.

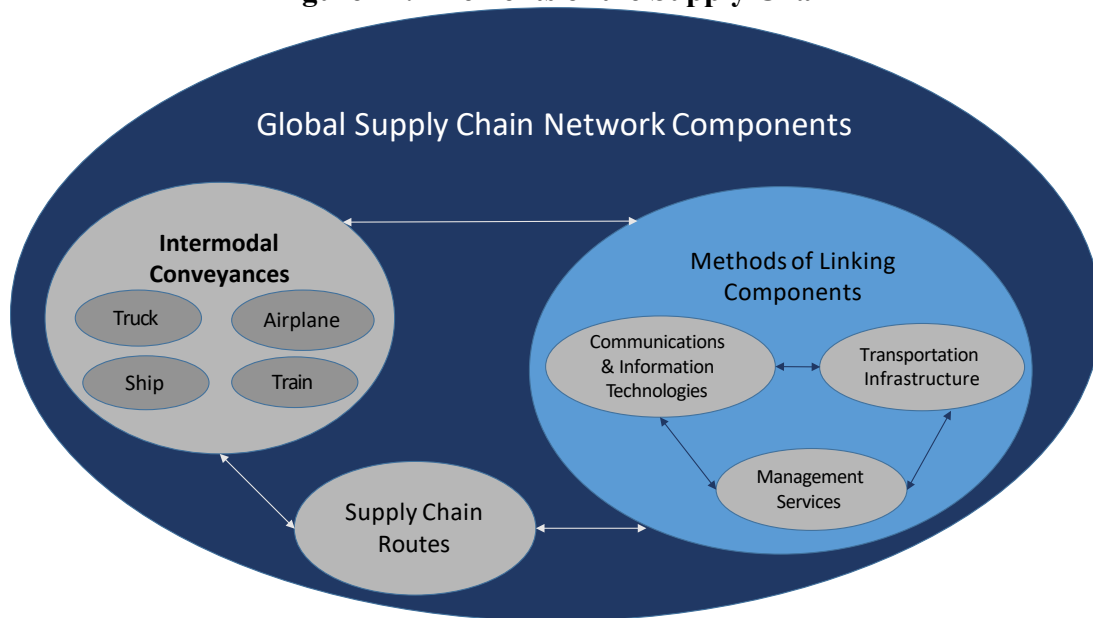
Because the global supply chain functions as an integrated conglomerate of processes, the global transportation community must work together to monitor how the transportation vulnerabilities that may affect the global supply chain work independently and collectively. Individual vulnerabilities could impact the entire intermodal network.

2020 Intermodal Transportation Security Plan

Securing the supply chain raises issues involving the security of infrastructure, facilities, carriers, people, cargo, and information. Figure 17 breaks out the elements of the supply chain (intermodal conveyances, supply chain routes, communications and information technologies, transportation infrastructure, and management services), and establishes the means of how the routes and conveyances link together to create a seamless interconnected intermodal system.

The transportation infrastructure is made up of the physical components of each transport mode and intermodal terminal, to include aircraft, vessels, vehicles, facilities, and equipment. Communication and technology services are the key data systems that provide communication and information, to include navigation services, which enable safe and efficient transport from one destination to another. Transportation management services are complex, with many stakeholders that manage the operations of various sectors within the global supply chain to facilitate the freedom of movement and free flow of commerce. The supply chain routes are the physical routes involved in the production and distribution of a commodity. Transportation conveyances move a commodity from one place to another. This framework, depicted in Figure 17, allows for the identification of cross-cutting trends, establishment of priorities, and the identification of needs across the components.

Figure 17: Elements of the Supply Chain



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.

2020 Intermodal Transportation Security Plan

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 if such a disruption coincided with another emergency, such as a natural disaster.

The complexity of the transportation network and open access to its many pathways increase the opportunity for terrorists to exploit the supply chain for nefarious purposes. While risk mitigation measures improve defenses and resilience, transportation elements of supply chains, by their nature, remain vulnerable to terrorist exploitation. Terrorists, for example, may exploit security vulnerabilities in supply chains to transport WMD, weapons, or IED precursors or components, or use vehicles, trains, vessels, or aircraft, including unmanned aircraft system or drones, as weapons themselves (such as in the 9/11 attacks or the recent spate of truck ramming incidents in Europe and the United States).⁹⁴ With drones becoming increasingly common, terrorists can use them to facilitate their criminal activities, including smuggling, surveillance, and disrupting the transportation sector.

Intermodal operations in major transportation gateway cities are critical pathways for many supply chains. Significant disruption in any one of these critical pathways 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.

The security practices and initiatives advanced by industry and government may be applied broadly to the Nation's domestic and international supply chains. However, 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 materials such as certain ores, minerals, and rare Earth elements
- Petroleum and energy products
- Medicines, medical supplies, and human organs
- Produce and perishable food
- Chemicals for defense industries, public health needs, and water sanitation

⁹⁴ 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).

2020 Intermodal Transportation Security Plan

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: Security planning and information sharing across subsectors and developing a continuity of operations plan facilitate the performance of essential functions during all-hazards emergencies or other situations that may disrupt normal operations.

Harmonization of international supply chain security protocols: Streamlining and harmonizing government processes and policies to improve uniformity of trade enforcement processes through ports of entry and ensure information sharing across subsectors.

State of good repair of transportation infrastructure, shipping hubs, and intermodal nodes: Building and maintaining resilient infrastructure that can adapt to changing conditions and withstand and rapidly recover from disruption.

Cyber and physical security of conveyances and facilities: Strengthen management of cyber and physical security risks to advance the security posture of cyber systems essential to intermodal transportation operations.

Cargo screening and inspection: Federal agencies and private industry employ a variety of screening and inspection capabilities to mitigate the risk of introducing dangerous items into transportation systems.

Credentialing, vetting, and access controls: Improved screening and vetting capabilities of personnel security assessments and credentialing programs.

2020 Intermodal Transportation Security Plan

II. Mitigation Programming

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 (for example, 24-hour advance manifest rule), cooperative arrangements with foreign customs organizations (for example, the Container Security Initiative), and international protocols through U.N. organizations such as the World Customs Organization and the Universal 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, CTPAT 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, CTPAT members are considered lower-risk, and CBP is able to focus on inspection of higher-risk shipments.⁹⁵

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 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.

⁹⁵ Risk-segmentation helps expedite low-risk trade and enables CBP to strengthen comprehensive trade enforcement by focusing enforcement resources on the shipments with the highest risk of containing unsafe or dangerous merchandise, and detecting fraudulent trade practices that undermine the competitiveness of compliant American industries. 2020 Vision and Strategy, CPB Strategic Plan, pg. 24.

2020 Intermodal Transportation Security Plan

III. Objectives, Activities, and Measuring Progress

The Intermodal Transportation Security Plan’s goals and objectives reflect the risk-based priorities and support the national objectives of the National Strategy for Global Supply Chain Security.⁹⁶ Figure 18 highlights the path forward to address unique intermodal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to intermodal transportation security.

Figure 18: Intermodal Transportation Security Goals

NSTS Goal 1	Manage risks to transportation systems from terrorist attack and enhance system resilience
<p>Objective 1.1:</p> <p>Manage risks from transportation vulnerabilities in vital supply chains.</p>	<p>Activity 1.1.1: Identify and assess key supply chain transportation assets and systems. (DHS/PLCY)</p> <p>Outcome: Improve prioritizing supply chain risks.</p> <p>Performance Measurement: Estimate percent completion of identification and assessment of priority supply chains. (DHS/PLCY)</p> <hr/> <p>Activity 1.1.2: Support state and local government to remediate physical security vulnerabilities of transportation operations to protect critical infrastructure.</p> <p>Outcome: Improve the reliability and resilience of critical supply chain nodes.</p> <p>Performance Measurement: Percentage of physical inspections completed of bridges noted within the National Bridge Inventory. (DOT/FHWA)</p>
<p>Objective 1.2:</p> <p>Encourage adoption of global supply chain transportation-related standards, regulations, guidelines, and best practices.</p>	<p>Activity 1.2.1: Implement the ISPS 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)</p> <p>Outcome: Reduce risk to the United States from substandard security at foreign ports.</p> <p>Performance Measurement: Percentage of trading partners assessed for effective anti-terrorism measures. (DHS/USCG)</p>

⁹⁶ <https://www.dhs.gov/national-strategy-global-supply-chain-security>.

2020 Intermodal Transportation Security Plan

NSTS Goal 2	Enhance effective domain awareness of transportation systems and threats
<p>Objective 2.1: Enhance federal analysis and sharing of transportation security supply chain information to improve situational awareness of terrorist threats.</p>	<p>Activity 2.1.1: 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. (DHS/CBP/USCG)</p> <p>Outcome: Use risk segmentation methods to inform scanning decisions.</p> <p>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. (DHS/CBP)⁹⁷</p> <p>-----</p> <p>Activity 2.1.2: Develop cybersecurity-related incident and vulnerability reporting guidance for transportation systems sector stakeholders in alignment with the NIST Cybersecurity Framework, the National Cyber Incident Response Plan, and applicable law. (DHS/CISA/DOT)</p> <p>Outcome: Increase in cybersecurity domain awareness.</p> <p>Performance Measurement: Percent of assessed transportation systems sector operators implementing the NIST Cybersecurity Framework. (DHS/CISA/DOT)</p>
<p>Objective 2.2: Strengthen and grow stakeholder partnerships and collaboration on supply chain resilience.</p>	<p>Activity 2.2.1: Streamlining security processes in collaboration with public and private sector partners to enhance U.S. economic competitiveness by enabling lawful trade. (DHS/CBP)</p> <p>Outcome: Reduce trade delays through security process improvements.</p> <p>Performance Measurement: Percent of imports compliant with applicable U.S. trade laws. (DHS/CBP)</p>
NSTS Goal 3	Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce
<p>Objective 3.1: Manage transportation risks in the global supply chain networks to promote the efficient flow of commerce.</p>	<p>Activity 3.1.1: Expand risk segmentation through advanced technology to enable low-risk trade and travel. (Automated Targeting System, Automated Manifest System, Air Cargo Advance Screening, and CTPAT)</p> <p>Outcome: Improve cargo flow to the United States through risk segmentation methods.</p> <p>Performance Measurement: Percent of cargo by value imported to the United States by participants in CBP trade partnership programs.</p> <p>-----</p>

⁹⁷ (ii) High-risk cargo. For cargo that CBP has identified as potentially high-risk, the carrier, after being duly notified by CBP, will be responsible for delivering the cargo for inspection/examination. When cargo identified as high risk has already been exported, CBP may demand that the export carrier redeliver the cargo in accordance with the terms of its international carrier bond (see § 113.64(m)(2) of this chapter).

2020 Intermodal Transportation Security Plan

NSTS Goal 3	Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce
	<p>Activity 3.1.2: Streamlining security processes in collaboration with public and private sector partners to enhance U.S. economic competitiveness by enabling lawful trade. (DHS/CBP)</p> <p>Outcome: Reduce trade delays through security process improvements.</p> <p>Performance Measurement: Percent of imports compliant with applicable U.S. trade laws. (DHS/CBP)</p>



Appendix E: Mandates for the Strategy



**Homeland
Security**

Transportation Security Administration

Legislative Language

The 2020 National Strategy for Transportation Security addresses requirements in legislation, executive orders, and departmental directives including, but not limited to, the following documents:

- *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 (2018)
- National Strategy for Counterterrorism (2011)
- National Strategy for Global Supply Chain Security (2012);
- NIPP 2013, *Partnering for Critical Infrastructure Security and Resilience*
- 2014 Quadrennial Homeland Security Review (2014)
- National Cyber Strategy (2018)

The IRTPA required the Secretary of Homeland Security to “develop, prepare, implement, and update” a National Strategy for Transportation Security.⁹⁸ 49 U.S.C. 114(s) states:

- (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.

⁹⁸ 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.

(4) Submissions of plans.

(A) In general. The Secretary of Homeland Security shall submit the National Strategy for Transportation Security, including the transportation modal security plans and any revisions to the National Strategy for Transportation Security and the transportation modal security plans, to appropriate congressional committees not less frequently than April 1 of each even-numbered year.

(B) Periodic progress report.

(i) Requirement for report. Each year, in conjunction with the submission of the budget to Congress under section 1105(a) of title 31, United States Code [31 USCS § 1105(a)], the Secretary of Homeland Security shall submit to the appropriate congressional committees an assessment of the progress made on

implementing the National Strategy for Transportation Security, including the transportation modal security plans.

(ii) Content. Each progress report submitted under this subparagraph shall include, at a minimum, the following:

(I) Recommendations for improving and implementing the National Strategy for Transportation Security and the transportation modal and intermodal security plans that the Secretary of Homeland Security, in consultation with the Secretary of Transportation, considers appropriate.

(II) An accounting of all grants for transportation security, including grants and contracts for research and development, awarded by the Secretary of Homeland Security in the most recent fiscal year and a description of how such grants accomplished the goals of the National Strategy for Transportation Security.

(III) An accounting of all—

(aa) funds requested in the President’s budget submitted pursuant to section 1105 of title 31 [31 USCS § 1105] for the most recent fiscal year for transportation security, by mode;

(bb) personnel working on transportation security by mode, including the number of contractors; and

(cc) information on the turnover in the previous year among senior staff of the Department of Homeland Security, including component agencies, working on transportation security issues. Such information shall include the number of employees who have permanently left the office, agency, or area in which they worked, and the amount of time that they worked for the Department of Homeland Security.

(iii) Written explanation of transportation security activities not delineated in the National Strategy for Transportation Security. At the end of each fiscal year, the Secretary of Homeland Security shall submit to the appropriate congressional committees a written explanation of any Federal transportation security activity that is inconsistent with the National Strategy for Transportation Security, including the amount of funds to be expended for the activity and the number of personnel involved.

(C) Classified material. Any part of the National Strategy for Transportation Security or the transportation modal security plans that involve information that is properly classified under criteria established by Executive order shall be submitted to the appropriate congressional committees separately in a classified format.

(D) Appropriate congressional committees defined. In this subsection, the term “appropriate congressional committees” means the Committee on Transportation and Infrastructure and the Committee on Homeland Security of the House of Representatives and the Committee on Commerce, Science, and Transportation, the Committee on Homeland Security and Governmental Affairs, and the Committee on Banking, Housing, and Urban Affairs of the Senate.

(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.

(6) Coordination.

In carrying out the responsibilities under this section, 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.

(7) Plan distribution.

The Secretary of Homeland Security shall make available and appropriately publicize an unclassified version of the National Strategy for Transportation Security, including its component transportation modal security plans, to Federal, State, regional, local and tribal authorities, transportation system owners or operators, private sector stakeholders, including nonprofit employee labor organizations representing transportation employees, institutions of higher learning, and other appropriate entities.



Appendix F: Supplementary Information



**Homeland
Security**

Transportation Security Administration

I. Acronyms

AMSC	Area Maritime Security Committee
ATS	Aviation Transportation System
BASE	Baseline Assessment for Security Enhancement
CTPAT	Customs-Trade Partnership Against Terrorism
CBP	U.S. Customs and Border Protection
CFR	Code of Federal Regulations
CIPAC	Critical Infrastructure Partnership Advisory Council
CSR	Corporate Security Review
CWMD	Countering Weapons of Mass Destruction Office
DOE	U.S. Department of Energy
DHS	U.S. Department of Homeland Security
DHS TRIP	Department of Homeland Security Travelers Redress Inquiry Program
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HMC	highway and motor carrier
HSPD	Homeland Security Presidential Directive
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
ISPS	International Ship and Port Facility Security
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
MTSA	Maritime Transportation Security Act
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NNSA	National Nuclear Security Administration
NSAS	National Strategy for Aviation Security
NSPTS	National Strategy for Public Transportation Security
NSRTS	National Strategy for Railroad Transportation Security
NSTS	National Strategy for Transportation Security
NTRS	National Transportation Recovery Strategy
PHMSA	Pipeline and Hazardous Materials Safety Administration
R&D	Research and Development
RSSM	rail security-sensitive material
SAM	Security Awareness Message
SCADA	Supervisory Control and Data Acquisition
STSAC	Surface Transportation Security Advisory Committee

TSA	Transportation Security Administration
TSSRA	Transportation Sector Security Risk Assessment
UAS	unmanned aircraft systems
USCG	U.S. Coast Guard
VBIED	vehicle borne improvised explosive device
WMD	weapon of mass destruction

II. Methodology

A. Plan Development

The Aviation and Maritime appendices may be divided into sub-modes. The Surface Security Plan appendix must be divided into four modal security plans to permit prioritization of risks across and within the traditional surface modal communities (49 USC 114(s)(1)(B)). Each plan will address the requirements in 49 USC 114(s) as explained above.

The modal security plans will be developed by the modes, using the 2018 NSTS as a baseline. The designated project leads will develop the sections of the 2020 NSTS to which they are assigned with the exception of the NSRTS and NSPTS. The Policy, Plans, and Engagement (PPE) Surface Division will update and incorporate the NSRTS and the NSPTS into the Surface modal plans, and execute the clearance process as appropriate.

Project leads will engage TSA's modal planners to review, update, or revise their respective plans, as necessary. The project team will develop the modal security plans by collecting information from modal planners. The modal planners will provide information requested by the project team leads via data calls.

B. Analytic Approach

The analysis for updating the NSTS and supporting plans will include the following steps:

1. Analytic Teams

TSA's Strategy, Policy Coordination, and Innovation (SP&I) office will facilitate meetings and discussions to ensure the priorities, objectives, activities, and measurement approaches are nationally focused. The analytic teams will consist of the modal planners and appropriate stakeholders who have equities in the respective subject areas. They will also facilitate the stakeholder engagement process.

2. Stakeholder Engagement

In accordance with legislation, TSA and DOT will "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."⁹⁹

Government Coordinating Councils and Sector Coordinating Councils are highly regarded as key strategic partners. Modal planners are encouraged to meet requirements for consultations with private sector stakeholder through established relationships with these councils. Advice received

⁹⁹ 49 U.S.C. § 114(s)(3)(A).

from the private sector through Critical Infrastructure Partnership Advisory Committee (CIPAC)-related councils is not restricted by the Federal Advisory Committee Act (FACA).¹⁰⁰

Modal planners are responsible for meeting this legislative requirement by engaging stakeholders as appropriate. To support engagement activities, modal planners may find it beneficial to maintain a record of the various groups in the community with whom they engage. Such a record will provide source material for inquiries, particularly during Office of Management and Budget, National Security Council staff, and congressional staff reviews, about the extent to which members of the “whole” community were involved.

Modal planners are encouraged to develop a communications matrix, similar to the example below, to record detailed communications activities. It is helpful for both planning and documenting the communications achieved during the engagement process. It also provides “data” for stakeholder engagement metrics.

Vehicle/ Media	Content	Stakeholder Group	Frequency	Comments
Scheduled NSTS meetings	<ul style="list-style-type: none"> Address planning challenges Provide guidance 	<ul style="list-style-type: none"> NSTS participants, others as appropriate 	As necessary	
Emails/iShare/HS IN	<ul style="list-style-type: none"> Informational emails Current versions Upcoming meetings 	<ul style="list-style-type: none"> NSTS participants, others as appropriate 	As necessary	
Transportation Sector Comments mailbox	<ul style="list-style-type: none"> NSTS updates/questions/concerns 	<ul style="list-style-type: none"> NSTS participants, others as appropriate 	On-going	

3. Literature Review

The literature review consists of identifying key documents by which the mode will establish the basis for risk-based priorities and risk-reduction/management activities. Commonly used documents are TSA Office of Intelligence and Analysis and DHS Office of Cyber and Infrastructure Analysis threat assessments; TSA Administrator's Intent; *FAA Reauthorization Act of 2018* (Pub. L. 115-254; October 5, 2018); White House national strategies, directives and executive orders; DHS strategies, plans, and directives; other assessments sources (for example, Office of the Director of National Intelligence, Domestic Nuclear Detection Office, U.S.

¹⁰⁰ CIPAC was established as a mechanism to directly support sectors’ interest to engage in public-private critical infrastructure discussions and participate in a broad spectrum of activities. CIPAC exempts partnership meetings from FACA.

Department of Defense, U.S. Department of State); and agency (for example, TSA and CBP) strategic documents, budget justifications, testimonies, and joint white papers. These sources are analyzed within the context of specific strategic goals and strategic outcomes and should help leaders make decisions on risk-based priorities.

4. Data Calls

Strategy and Plans Branch will solicit updates from modal planners through two modal-specific data calls. The data calls are constructed to build upon each other. Data call 1 will assist in updating the 2018 NSTS Base Plan; data call 2 will assist in updating the Modal Security Plans, as necessary, to align with the Base Plan. The data calls are logically sequenced to encourage consideration of modal strategic approaches in the following order: 1) a description of assets to be protected, 2) risks to those assets, and 3) risk-based priorities to address the risks.

a. Data Call 1: Update of 2018 NSTS Base Plan

The first data call requested an update to the 2018 NSTS base plan. This update of the 2018 NSTS, which was delivered to Congress on April 4, 2018, will continue the effort to “streamline” the strategy to address specific requirements in the legislation. It will include changes, if necessary, to the strategic environment, challenges, and path forward. The modal planners will consider the challenges and impacts to their respective mode and recommend feasible solutions.

b. Data Call 2: Update of Modal Security Plans

The second data call will request an update to the Modal Security Plans to include all key components—the modal profile, risk profile, and risk-based priorities, objectives, activities, and performance measures found in the 2018 NSTS.

Modal Profile: The modes will identify the assets that need to be protected in the interests of national security (49 USC 114(s)(3)(A)). This update requires revisions to reflect recent changes in the risk environment and other necessary modal changes.

Risk Profile and Risk-Based Priorities: The strategic environment included in the base plan will inform the risk profile and the risk-based priorities, and will be provided to the modal planners for consideration in completing this data call. Generally, risk-based priorities are determined through analyses of source materials (congressional or executive direction, legislation, risk assessments, threat assessments, and gap analyses) and other factors as appropriate.

Objectives and Activities: Modal planners must document the basis for risk-based priorities, objectives, and activities separately from the NSTS, following these requirements:

- Each objective must be expressed as an outcome.
- The modal objectives must be achieved by activities conducted over the 4-year planning cycle.
- Each activity must have milestones indicating the completion of key events or activities to show progress implementing the activity.
- Each activity must have an outcome-focused performance measure with a target that will indicate the effectiveness or efficiency of the activity.

The record must include the sources used and rationale to defend decisions during audits, budget development, and other processes.

Performance Measures: Modal planners must update any activity or measure that is not feasible or quantifiable with data, and identify target or baseline for meeting the performance measure. Performance measures should be developed by the data owner. As a reminder, if an activity is in the NSTS Modal Security Plan, then it must have performance measures that are reported on in the Annual Report to Congress.

c. Definition of Terms

- Performance measure: Demonstrates that the activity is achieved by quantifying its effectiveness or efficiency.
- Measure description: Explains what the measure assesses, how it will be quantified, and why it is useful.
- Data source: Documents the data (either quantitative or qualitative) including any relevant systems and reports used to measure the results, and how the necessary data is accrued.
- Supporting rationale: Discusses any result that does not meet the performance target, or provides other information to the reader to explain the performance result.

III. Roles and Responsibilities

A. Federal Government

DHS provides strategic security planning and guidance, promotes a national unity of effort using the whole-of-government approach, 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 U.S. Department of State, the U.S. Department of Justice, the U.S. Department of Energy, the U.S. Department of Defense, the U.S. Department of Commerce, and the U.S. Department of Agriculture. In carrying out these responsibilities, the Federal Government:

- Evaluates national capabilities, opportunities, and challenges in securing 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
- Provides grant funding to support risk management activities

Transportation Security Administration

TSA is responsible for securing the U.S. transportation systems while ensuring the freedom of movement for people and commerce. TSA employs a layered, risk-based approach, working closely with stakeholders in aviation, freight rail, mass transit and passenger rail, highway and motor carrier, and pipeline sectors, as well as the partners in the law enforcement and intelligence community.

United States Coast Guard (USCG)

The USCG is responsible for an array of maritime duties, from ensuring safe and lawful commerce to performing rescue missions in severe conditions. The USCG provides information in regards to defending America's borders and protecting the maritime environment.

The USCG's role in national defense and anti-terrorism is a cornerstone of homeland security efforts to protect the country from the ever-present threat of terrorism. The USCG carries out three basic roles, which are further subdivided into eleven statutory missions. The three roles are maritime safety, maritime security, and maritime stewardship.

Countering Weapons of Mass Destruction Office (CWMD)

The Countering Weapons of Mass Destruction Office (CWMD) enhances and coordinates DHS strategic and policy efforts with Federal, State, local, tribal, and territorial (FSLTT) governments and the private sector to prevent WMD use against the homeland and promote readiness against chemical, biological, radiological, nuclear and health security threats. CWMD has the primary authority and responsibility, in support of DHS Operational Components, to research, develop, acquire, and deploy operationally effective solutions to protect the Nation from CBRN weapons and health security threats.

Cybersecurity and Infrastructure Security Agency (CISA)

The Cybersecurity and Infrastructure Security Agency is an operational component within DHS. CISA builds the national capacity to defend against cyber-attacks and works with the Federal Government to provide cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies. CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers technical assistance and assessments to federal stakeholders, as well as to infrastructure owners and operators nationwide. In addition, the agency enhances coordination, tools, guidance, and public safety interoperable communications at all levels of government, to help partners across the country develop their emergency communications capabilities.

U.S. Department of Energy (DOE)

DOE plays an important and multifaceted role in protecting national security, including work against the proliferation of WMD. Its national labs provide both subject matter expertise and personnel with unique skills to help understand a wide array of threats and vulnerabilities to the aviation domain. Additionally, the National Nuclear Security Administration (NNSA) is the United States Government's primary capability for radiological and nuclear emergency response and for providing security to the Nation from the threat of nuclear terrorism. NNSA coordinates with other agencies whose roles include nuclear or radiological emergency response functions.

U.S. Department of Commerce

The U.S. Department of Commerce, in collaboration with DHS and other relevant federal departments and agencies, engages private sector, research, academic, and government organizations to improve security for technology and tools related to cyber-based systems. It enables the timely availability of industrial products, materials, and services to meet homeland security requirements.

U.S. Department of Transportation

The mission of the DOT is to ensure our Nation has the safest, most efficient and modern transportation system in the world, which improves the quality of life for all American people and communities, from rural to urban, and increases the productivity and competitiveness of American workers and businesses. The DOT oversees and administers a wide range of transportation programs, policies, and regulations for both aviation and surface transportation.

U.S. Department of State

The U.S. Department of State promotes U.S and international best practices that protect the homeland, as well as U.S. citizens and interests overseas, through bilateral and multilateral diplomacy, programs, and capacity building, to include transportation and border security policies and processes. State, in joint coordination with DOT, also has responsibilities with respect to negotiating, approving, and interpreting international agreements, including with respect to transportation security.

B. State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial government entities are the first to respond to terrorist incidents. Consequently, they are best positioned to address specific homeland security needs and to assume the lead for local preparedness. They also 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.

State and territorial governments establish partnerships, facilitate coordinated information sharing, and enable planning and preparedness for critical infrastructure security and resilience within their jurisdictions. They provide information to DHS, as part of the grants process or through homeland security strategy updates, regarding state or territorial priorities, requirements, and critical infrastructure-related funding needs.

Local governments provide critical public services and functions in conjunction with private sector owners and operators. Local authorities typically shoulder the weight of initial response and recovery operations until coordinated support from other sources becomes available, regardless of who owns or operates the affected asset, system, or network.

Tribal government roles and capabilities generally mirror those of state and local governments. They are responsible for the public health, welfare, and safety of tribal members, as well as the continuity of essential services under their jurisdiction.

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 state, local, tribal, and territorial government entities. Since the 9/11 attacks, owners and operators have undertaken significant steps, many voluntary, to reduce security risks. Those steps include:

- Conducting risk assessments
- Developing security plans, employee training, and exercise programs
- Establishing business continuity plans and programs that sustain critical transportation functions during and following a security-related incident
- Participating in coordination bodies and mechanisms such as Sector Coordinating Councils, Aviation Security Advisory Committee, Peer Advisory Groups, and Area Maritime Security Councils

IV. 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 of 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)

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, 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)

Homegrown Violent Extremist. A person of any citizenship who has lived and/or operated primarily in the United States or its territories who advocates, is engaged in, or is preparing to engage in ideologically-motivated terrorist activities (including providing support to terrorism) in furtherance of political or social objectives promoted by a foreign terrorist organization, but is acting independently of direction by a foreign terrorist organization. HVEs are distinct from traditional domestic terrorists who engage in unlawful acts of violence to intimidate civilian populations or attempt to influence domestic policy without direction from or influence from a foreign actor.

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

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 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 to life, information, operations, the environment, 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)