Appendix A: Aviation Security Plan

Homeland Security

I. Introduction

A. Overview

The Aviation Security Plan addresses the security of the Aviation Transportation System (ATS) through the four main components of the mode: commercial airlines, airports, general aviation, and air cargo.[1] Within these components, there are many aviation support functions and activities providing services as defined in the aviation ecosystem.[2] 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 malicious use of UAS. Any disruption of critical infrastructure elements in the aviation domain could create ripple effects throughout the entire system or to other critical infrastructure sectors. 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.[3,4] 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] 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.

[2] 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, aircrafts, airlift, actors, and aviation management. The National Airspace System falls under aviation management within the aviation ecosystem.

[3] NSPD-47/HSPD-16.

[4] 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.

1) Modal Profile

In the interest of national security and commerce, aviation assets and systems needing protection from attack by adversaries include, but are not limited to: the air traffic control system, domestic airports, foreign airports serving as the last points of departure to the United States, commercial airliners and cargo aircraft operating in, to, and from the United States, air cargo, general aviation, aircraft manufacturing and maintenance industries, training centers, pilot and aviation maintenance technician schools.[5]

Risk management strategies in the Aviation Security Plan address physical, human, and cyber elements of aviation activities and their supporting services, as necessary, to protect life and property and to prevent unauthorized access or unlawful interference which may cause disruption of the ATS.

The components in **Figure 3** identify the main sub-modal aviation communities and the organizational approach to security planning and programming.[6]

Figure 3: Components of the Aviation Mode

Air Cargo	Air cargo means 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[7]. The air cargo operations serving the U.S. are made up of over 300 domestic and foreign air carriers and all-cargo carriers, and over 4,000 indirect air carriers.
Commercial Airlines	Commercial airlines are those that engage in regularly scheduled passenger and cargo service or public charter operations, including domestic aircraft operators and foreign air carriers flying within, from, to, or over the U.S. 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.[8] There are approximately 440[9] airports in the U.S. 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 by the International Civil Aviation Organization as all civil aviation operations other than scheduled air services and nonscheduled air transport operations for remuneration or hire. General aviation operations also exclude military operations.

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

[6] The components of the aviation mode incorporate the protection of the aviation ecosystem.

[7] 49 CFR 1540.5 – Definition of "Cargo."

[8] 49 U.S.C. § 47102(7).

[9] Numbers fluctuate due to seasonality.

Flight Schools, Training Centers, and Aviation Maintenance Technician 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. Training centers are organizations governed by the applicable requirements that provides training, testing, and checking under contract or other arrangement to airmen subject to the requirements. educational facility certificated by the FAA, under 14 CFR part 147, to train students in the knowledge and skills required for careers in the aviation maintenance industry. This will also include Aviation Maintenance Training Schools that are educational facility certificated by the FAA, under 14 CFR part 147, to train students in the knowledge and skills required for careers in the aviation maintenance industry.
Air Traffic Control	A service operated by appropriate authority to promote the safe, orderly, and expeditious flow of air traffic.
Repair Stations	A maintenance facility that has a certificate issued by the FAA under Title 14 of the Code of Federal Regulations (14 CFR) Part 145 and is engaged in the maintenance, inspection, and alteration of aircraft and aircraft products.

2) Risk Profile

The risk profile for the aviation mode of transportation is dominated by international terrorism, but also includes domestic terrorism.[10] The greatest threat to aviation security remains Improvised Explosive Devices (IEDs). Emerging technologies, such as UAS and 3D printing technology, provide opportunities for terrorists to attack aviation targets in ways that are difficult to detect. These threats are not listed in prioritized order.

International and Domestic Terrorists: Terrorist attacks on transportation assets often incorporate 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 vehicle borne improvised explosive devices (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 ongoing 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 possibility of being detected. Returning foreign fighters create substantial risks to the homeland when they travel to other

[10] Risk profiles and scenarios sources include TSSRA and TSA aviation assessments.

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. UAS can be equipped with cyber payloads to enable data theft, network infiltration, or delivery of malicious code to victim systems. Small UAS, in particular, can be launched from anywhere and can be difficult to detect by traditional surveillance (radar). Efforts to develop UAS detection and mitigation systems, as well as minimize the safety risks the use of such systems may create for other users of the NAS, continue.

Cyber: The Aviation mode increasingly relies on cyber-based systems and infrastructure. More and more important daily activities, such as scheduling, messaging, maintenance, positioning, navigation, and timing rely on a dependable and resilient cyber environment for safety, security, efficiency, and convenience.

The demand for all parts of the aviation ecosystem is dynamic, and it typically increases annually. As the aviation mode adjusts to volume changes, so do the threats to cyber-based systems. A wide range of cyber threats actors target both the cyber environment of the aviation ecosystem and its supporting infrastructure.

The cyber threat landscape is evolving and continues to adapt and change. Many cyber threats can be mitigated through awareness and best practices in cybersecurity. Defending the aviation ecosystem against these threats requires addressing both the technical and social elements of the cyber threat landscape.

The aviation risk profiles listed in **Figure 4**, informed by TSSRA and other intelligence analyses, provide the basis for risk-based aviation security priorities.

Figure 4: Aviation Risk Profiles

Air Cargo Risk Profile	Air cargo risks are magnified by the vast number and diversity of shippers, cargo handlers, and transportation carriers across modes in the global supply chain. Air cargo is transported on a wide range of aircraft, to include passenger aircraft and all cargo aircraft, and can be tendered to aircraft operators via indirect air carriers. The air cargo industry transports a wide range of cargo, including express shipments, heavy freight, vehicles, machine parts, medical supplies, and cold chain shipments. In addition, multinational corporations are vertically integrating and blending traditionally separate roles, adding further complexity to the shipping system. The presence of cargo shipments on passenger carriers and all-cargo carriers increases the security risk level of the aircraft. 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 point-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 travel 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 if actors were to gain access to the facility. 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. Unauthorized UAS activity in key airport locations could cause an outsized disruption to airport traffic or deliver malicious payloads (for example, UAS carrying IED to aviation fuel farms), evading traditional physical security measures.
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.
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 prohibited items into transportation venues. Screening and advance information technologies help mitigate the risk of introducing TSA prohibited items into the Aviation Transportation System (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.

Insider Risk: 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, employee screening, credentialing programs, and detecting insider risk activities.

Mitigating Terrorist Travel: Mitigating terrorist travel is a top priority. The strategic approach to mitigating 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.[11]

[11] National Strategy to Combat Terrorist Travel, pp 14 & 15. National Strategy to Combat Terrorist Travel (fas.org).

Protecting Privacy, Civil Rights, and Civil Liberties During Screening: The security screening process must respect the unique personal circumstances of travelers and transportation systems sector workers, 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 include travelers with limited English proficiency, travelers wearing religious/ethnic headwear/clothing, transgender/gender diverse travelers, and other travelers who may need to be screened using modified procedures. These modified special procedures will continue to preserve security while accommodating the unique needs of the traveler.

Cybersecurity: Implementing a cybersecurity framework that is both risk-based and threat-informed is critical. Such a framework is essential for providing organizations with a structure to assess and improve their ability to prevent, detect, and respond to cyber incidents. Cybersecurity programs should use risk-based decisions to protect a wide range of critical infrastructure. Such infrastructure includes: 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); information and operational technology systems critical to safe, secure, and efficient aviation operations, and water/wastewater systems.

Responding to and Countering[12] UAS and Autonomous Systems Threats in an Airport Environment: The NSTS recognizes the need to assess and adapt to the mission area of the UAS and autonomous conveyances systems. UAS and autonomous systems are transformative innovations. However, they pose both defense and national security challenges. The NSTS emphasizes the activities, processes, and systems required to respond to potential threats posed to the transportation systems sector by UAS and autonomous conveyances systems. Federal departments and agencies will assist transportation system owners and operators to prepare for and respond to UAS threats.

Preparedness: Developing a preparedness program in advance is integral to the successful management of any incident. In direct alignment of its strategy, TSA established a preparedness program that enhances its ability to advance global transportation security standards, as well as respond to threats and mitigate the risks to the safety and security of its workforce, mission, and the transportation systems sector. The approach establishes six foundational elements for TSA to achieve effective incident readiness and response efforts through a continuous preparedness cycle. These elements include: planning, organizing, training, exercise, equipping, and evaluating to improve processes).

[12] TSA requires additional statutory authorities to persistently counter and mitigate UAS threats in all modes of transportation.

II. Objectives, Activities, and Measuring Progress

The Aviation Security Plan's goals and objectives reflect the risk-based priorities. **Figure 5** highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national aviation security. This approach makes clear that no one government or agency can carry out a national security mission independently.

Figure 5: Aviation Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.1: Improve physical and cybersecurity of domestic aviation critical infrastructure.	**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])[13] **Outcome:** Reduction in vulnerability to potential insider threats from aviation workers. **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)
	Activity 1.1.2: Assess potential cybersecurity vulnerabilities of commercial aircraft. (TSA, CISA, and FAA) **Outcome:** Identify cyber vulnerabilities that may affect safe operation of commercial aircraft to support the FAA's, aircraft and other aviation manufacturers, and aircraft operators' analysis of potential risks to safety of flight and the development of appropriate risk reduction measures, as needed. **Performance Measurement:** As a part of the Aviation Cyber Initiative (ACI), initiate a cyber-risk reduction pilot program at the Idaho National Laboratory (INL). The pilot program will assess aircraft avionics for potential cybersecurity vulnerabilities using a newly developed, organic assessment capability based at the INL. (TSA and FAA)
	Activity 1.1.3: Assess potential cybersecurity vulnerabilities of airports. (TSA, CISA, and FAA)

[13] The Rap Back service allows authorized agencies to receive notification of activity on individuals who hold positions of trust (for example, schoolteachers, 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.

NSTS Goal 1	Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience
	Outcome: Identify cyber vulnerabilities that may affect safe operation of commercial airports to support the FAA, TSA, and other airport operators' analysis of potential risks to safety and security and the development of appropriate mitigation measures as needed. **Performance Measurement:** Percentage of organizations that have implemented at least one airport cybersecurity enhancement after receiving a vulnerability assessment or survey. (CISA and TSA) --- **Activity 1.1.4:** Assess UAS-related risks in the environs of commercial airports. (DHS/TSA/DOT/FAA) **Outcome:** Identify, track, report, and respond to UAS threats and vulnerabilities affecting safe, secure, and efficient operations at commercial airports. **Performance Measurement:** Percentage of UAS-specific Vulnerability Assessments conducted at commercial airports having resulted in implementing at least one UAS risk reduction countermeasure. (DHS/TSA)
Objective 1.2: Improve capabilities to prevent, protect, mitigate, respond to, and recover from terrorist attacks throughout the aviation community.	**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) **Outcome:** Reduction in dangerous articles introduced into the aviation system. **Performance Measurement:** Track system effectiveness using covert testing results to identify trends and vulnerabilities over time. (DHS/TSA)
Objective 1.3: Enhance international aviation security risk management strategies.	**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) **Outcome:** International policies and aviation security programs support U.S./DHS objectives to improve aviation security worldwide. **Performance Measurement:** Percent of foreign last point of departure airports where TSA has contributed to improving aviation security standards. 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 mitigation strategy for Man-Portable Air Defense Systems, FAM agreements, capacity development, conducting needs or risk assessments, and collaboration with DHS towards becoming preclearance airports. (DHS/TSA) --- **Activity 1.3.2:** Assess compliance with security measures required for service to the U.S. (DHS/CBP/TSA)

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
	Outcome: Identify compliance or noncompliance with security measures required for service to the U.S. **Performance Measurement:** Percentage of aviation security vulnerabilities which are closed through assessment and inspection activities. (DHS/TSA) --- **Activity 1.3.3:** Scan international inbound air cargo shipments entering the U.S. to detect radiological or nuclear threats. (DHS/CBP/CWMD) **Outcome:** Reduction of the risk of illicit radiological or nuclear agents entering the U.S. **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)
Objective 1.4: Increase security technology capability to respond to known and emerging threats.	**Activity 1.4.1:** Leveraging TSA work to harmonize standards internationally and improve the participation of aviation industry stakeholders 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) **Outcome:** Increase the participation of aviation industry stakeholders in processes to identify security capability gaps and develop solutions on a global scale. **Performance Measurement:** Percentage of aviation industry stakeholders participating in the R&D process to raise global detection and screening capabilities. (DHS/TSA)
NSTS Goal 2	**Enhance effective aviation domain awareness of transportation systems and threats**[14]
Objective 2.1: Improve quality in the sharing of intelligence information and products for government, industry, and public awareness.	**Activity 2.1.1:** Enhance the quality and applicability of intelligence sharing with security partners. (DHS/TSA and industry) **Outcome:** Improved quality and applicability of intelligence shared with customers. **Performance Measurement:** Percentage of annual customer surveys indicating TSA intelligence information helps the customer organization accomplish its mission and objectives. (DHS/TSA)

[14] NSAS, 2018.

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.	**Activity 3.1.1**: Resolve security risks of high-risk cargo identified by the Air Cargo Advance Screening (ACAS) program, by requiring enhanced screening of all inbound air cargo shipments targeted with a referral for screening prior to loading onto aircraft destined for the United States. (DHS/CBP and DHS/TSA) **Outcome:** Enhanced freedom of movement of low-risk cargo. **Performance Measurement:** Percentage of cargo shipments targeted by the Air Cargo Advance Screening Program that returned a Referral for Screening (RFS), which would require that regulated aircraft operators or foreign air carriers ensure enhanced screening measures, in accordance with their security program requirements, were applied before loading at the last point of departure. (DHS/TSA) --- **Activity 3.1.2:** Provide expedited aviation security screening for trusted travelers. (DHS/CBP and DHS/TSA) **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. **Performance Measurement:** The percentage of travelers who receive TSA PreCheck screening with a Known Traveler Number. (DHS/TSA)

III. Aviation Operational Recovery Plan

Transportation modal security plans should include an operational recovery plan to expedite the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident.[15]

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 National Strategy for Aviation Security (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."[16]

In concert with the federal recovery plans, airport and air carrier security programs required under federal regulation must contain emergency response procedures and contingency plans. The range of incidents may include scenarios identified in the Aviation Risk Profile.[17] [18]

.

[15] 49 U.S.C § 114(s).

[16] Aviation Transportation System Recovery Plan, 2018.

[17] 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.

[18] 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.

Appendix B: Maritime Security Plan

Homeland Security

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 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, philanthropic, academia, foreign governments; and international operators are vital partners in the collaborative effort to secure the system and ensure its resilience.

1) Modal Profile

The following federal agencies are responsible for regulatory oversight of the Maritime Transportation System (MTS):

- DHS (USCG, TSA, CBP, CISA, and the FEMA Port Security Grant Program (PSGP))
- DOT Office of the Secretary of Transportation and Maritime Administration (MARAD)
- DOD Army Corps of Engineers

The MTS is an integrated network that consists of 25,000 miles of coastal and inland waters and rivers serving 361 ports.[19] It supports $5.4 trillion dollars of economic activity each year and accounts for the employment of more than 30 million Americans.[20] The maritime transportation of cargo is considered the most economical, environmentally friendly, and efficient mode of

[19] https://www.dco.uscg.mil/Our-Organization/Assistant-Commandant-for-Prevention-Policy-CG-5P/Marine-Transportation-Systems-CG-5PW/Maritime-Commerce/.
[20] https://www.maritime-executive.com/article/u-s-port-economic-impact-rises-dramatically.

freight transport. As the economic lifeblood of the global economy critical to the U.S. national interests, the MTS connects U.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 U.S. economy, national security, execution of U.S. Campaign Plans, and sustaining national transportation of goods. Fifty-one of those 56 strategic ports are civilian owned. Twenty-four 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.[21] Eighteen of the 24 ports in the NPRN are civilian seaports and six are military seaports. From 2001-2019, over 90 percent of war winning materials flowed through these ports in support of overseas contingency 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 U.S. 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 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 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.

[21] Jones Act | Transportation Institute.
Maritime Security Act of 1996: H.R.1350 - 104th Congress (1995-1996): Maritime Security Act of 1996 | Congress.gov | Library of Congress.

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.

2) Risk Profile

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.

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 U.S. 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 U.S. borders.

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 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 U.S. 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;[22] 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

[22] 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.

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 (IT) infrastructure, maritime OT infrastructures, and maritime resident data, including the internet, the electromagnetic spectrum (predominately radio frequency spectrum), and any telecommunications networks (for example, 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, 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 (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 (for example, ICS) rely on precision, navigation, and timing 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.[23]

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.[24] 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, for example, 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.

Evolving/Emerging Technology: The shipping industry's rapid increase in the development and use of evolving and emerging technologies has the potential to present significant risks of new types of casualties that can cause considerable damage. The two biggest risks that need a mitigation strategy are the use of new fuels and shipping automation.

In April 2018, the International Maritime Organization laid out its strategy for the shipping industry to reduce its total greenhouse gas emissions at least 50 percent by 2050, from its 2008 levels. This goal has led to a big push in multiple parts of the transportation systems sector to decarbonize marine transportation. Emerging technologies that use new energy sources can both reduce their carbon footprint and at the same time pose greater risk than traditional fuels currently in use.

Newer vessels that run on hydrogen gas will require an infrastructure for delivery of these fuels. Most de-carbonized fuels that are potentially being proposed for use because of their low carbon rate are extremely dangerous both for their potential volatility and as inhalational hazards. Hydrogen is one example of a decarbonized fuel. Hydrogen is very flammable and explosive. Another type of fuel is ammonia. The Centers for Disease Control and Prevention states that ammonia is the second most hazardous gas after chlorine.

The Maritime Industry is looking at new and emerging technologies to automate electronic control systems, thereby reducing manning throughout the entire industry to include supply chain, terminal, port and shipboard operations, which utilize both fully automated and semi-automated systems. The new instrumentation on these vehicles, vessels and IT/OT systems will

[23] Transportation Statistics Annual Report: https://www.bts.gov/tsar.

[24] "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).

monitor their current status while looking for leading indicators and future problems, ultimately heading to predictive analysis. This means that human beings will no longer be required to be in an engine room, bridge watch or lookout; however, the distance to these automated maritime vessels may prevent them from being able to quickly respond in the event of a problem.
As you can see from the above information, mitigation strategies must be developed to prevent catastrophes for the risks, new fuels, and automated shipping technologies pose.

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.

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.[25] **Figure 6** 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 6: Maritime Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, 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 Security and Response Operations (MSRO). (DHS/USCG) **Outcome:** Reduce risks of terrorist planning and precursor activities. **Performance Measurement:** Percent of coordinated anti-terrorism activities contained in Port Tactical Activity Plans that were executed. (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:** Percent risk reduction of coordinated anti-terrorism activities throughout the Maritime Transportation System. (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)

[25] https://www.hsdl.org/?abstract&did=456414.

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.2: Reduce security vulnerabilities and improve preparedness throughout the Marine Transportation System.	**Activity 1.2.1:** Assess ISPS Code implementation in foreign ports that receive ships destined for the U.S. (DHS/USCG) **Outcomes:** Assess security (identify risks) at foreign ports serving ships destined for the U.S. **Performance Measurement:** Percentage of trading partners assessed. (DHS/USCG)
	Activity 1.2.2: Scan containerized cargo for illicit radiological or nuclear material. (DHS/CBP/CWMD) **Outcome:** Reduce the risk of illicit radiological or nuclear material entering the U.S. **Performance Measurement:** Percentage of containerized cargo conveyances that pass-through radiation portal monitors at seaports of entry per 6 U.S.C 982b. (DHS/CBP)
NSTS Goal 2:	**Enhance effective domain awareness of MTS and threats**
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.	**Activity 2.1.1:** Enhance resilience of cyber systems through implementation of the National Cybersecurity Strategy, exercises, guidance, assessments, and expansion of cyber intrusion detection and remediation technology. (DHS/USCG/CISA) **Outcome:** Improve awareness of and action to reduce the risk of cyber threats or malware. **Performance Measurement:** Percentage of the Area Maritime Security Plans that have been approved and implemented for cyber-related risks. (DHS/USCG)
	Activity 2.1.2: Participate in and materially support the development of a national Maritime Domain Awareness tool as defined in the Maritime SAFE Act[26] (DHS, TSA, USCG) **Outcome:** Improve whole-of-government Maritime Domain Awareness and information sharing **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)

[26] https://www.govtrack.us/congress/bills/116/s1269.

NSTS Goal 2:	**Enhance effective domain awareness of MTS and threats**
Objective 2.2: Improve Marine Transportation System stakeholder participation in the risk management process for security and resilience prioritization and programming.	**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) **Outcome:** Improve risk-based design of port exercises. **Performance Measurement:** Percentage of security exercises that include use of MSRAM data. (DHS/USCG)

NSTS Goal 3:	**Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce**
Objective 3.1: Collaborate with international partners to increase the reliability of the global supply chain.	**Activity 3.1.1:** Apply risk segmentation methods to evaluate cargo for expeditious clearance. (DHS/CBP) **Outcome:** Secure and expedite trade. **Performance Measurement:** Percentage of cargo by value imported to the U.S. by participants in CBP trade partnership programs. (DHS/CBP)

III. Maritime Operational Recovery Plan

Transportation modal security plans should include an operational recovery plan to expedite the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident.[27]

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

[27] 49 U.S.C § 114(s).

Security (NSMS).[28] 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.[29] 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.[30] 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,[31] 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 maritime trade. Actual or potential events include all hazards such as natural disasters, transportation security incidents, major maritime incidents, declaration of an Incident of National Significance, 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.

[28] 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.

[29] 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.

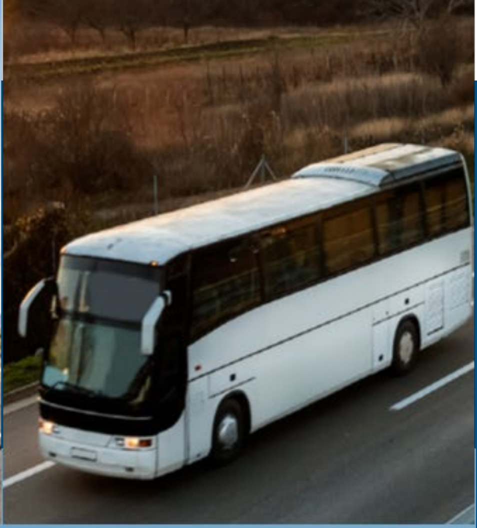
[30] https://www.dhs.gov/search?goog=Maritime%20Infrastructure%20Recovery%20Plan. Accessed February 4, 2022.

[31] https://www.dhs.gov/global-motr-coordination-center-gmcc.

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 (MIRP)-related activities.
- Support Presidential Policy Directive-18, National Strategy for 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), the National Maritime Transportation Security Plan, and the Maritime Infrastructure Recovery Plan (MIRP) to provide guidance for the recovery of the MTS and cargo flow.



Appendix C: Surface Security Plan

Homeland
Security

Surface Transportation Overview

The Surface Security Plan fulfills a requirement established by the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) to address the threats, vulnerabilities, and consequences for transportation assets that could be at risk from attack or disruption by terrorists or other hostile forces.[32] 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 7**.

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.[33] 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 analysis;
- Identification and application of research and development practices and technologies that can be leveraged to enhance security effectiveness; and
- Other actions such as the administration of security grant funding.

[32] 49 U.S.C. § 114(s).
[33] 6 U.S.C. § 1133.

Figure 7: 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 34 million riders daily and nearly 10 billion unlinked passenger trips in 2019.[34] Amtrak and Alaska Railroad provide the Nation's only long-distance passenger rail. Amtrak carried almost 16.8 million passengers in FY 2020.[35]
Freight Rail	Includes the 140,000-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.[36]
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.
Pipeline	Includes more than 2.8 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.[37] Above ground assets of note include compressor stations, pumping stations, and liquid and natural gas (LNG) facilities.

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 8**.

These seven risk-based priorities provide the foundation for supporting objectives and activities shown in **Figures 9**, **10**, **11** and **13**. 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 risks identified in each mode's risk profile and risk scenario sections.

[34] https://www.apta.com/news-publications/public-transportation-facts/.

[35] The American Public Transportation Association published, in fiscal year (FY) 2020, Amtrak service and ridership was significantly impacted by the COVID-19 pandemic. FY 2020 ridership decreased by 48 percent (to 16.8 million trips) compared to FY 2019. Ridership on the Northeast Corridor decreased by 51 percent of 6.1 million trips. https://www.apta.com/wp-content/uploads/APTA-2021-Fact-Book.pdf.

[36] https://www.aar.org/wp-content/uploads/2020/08/AAR-Railroad-101-Freight-Railroads-Fact-Sheet.pdf.

[37] https://www.phmsa.dot.gov.

Figure 8: 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 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 an attack, including, but not limited to, physical and cyber-attacks conducted by terrorists and nation-state actors, and test the effectiveness of security programs by identifying gaps in their preparedness measures.
Cybersecurity and critical infrastructure protection	Enhance the protection of the Transportation Systems Sector's critical infrastructure through analysis of current cyber-threats, identification of existing cyber-vulnerabilities, and development of cyber-risk mitigation steps to be shared through engagement with industry trade associations, working groups, councils, and advisory committees; to enhance awareness and preparedness of and response to attacks against both Information Technology (IT) and Operational Technology (OT) networks and systems of the Transportation Systems Sector.
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 first responders 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 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 safe 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.

DHS through TSA has the lead for surface transportation security; other federal departments contributing to surface transportation systems sector security efforts include additional DHS components (like CISA, FEMA, DHS Intelligence and Analysis, the USCG), DOT (Federal Transit Administration, Federal Railroad Administration, the Pipeline and Hazardous Materials Safety Administration [PHMSA], Federal Highway Administration, Federal Motor Carrier Safety Administration [FMCSA]), FBI, Federal Energy Regulatory Commission (FERC), and U.S. Department of Energy (DOE).

Federal Government responsibilities include:

- Assessing intelligence to identify potential threats to transportation security from nation-states, terrorists and other individuals. 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;
- Collaborating across Government Coordinating Councils; and
- Providing technical assistance to surface transportation owner/operators.

State, Local, Tribal, and Territorial Government Entities

State, local, tribal, and territorial (SLTT) government entities are generally the first to respond to terrorist and other security incidents involving surface transportation. Consequently, SLTT government entities must be engaged in identifying and addressing specific transportation security needs as well as leading local preparedness efforts.

SLTT responsibilities include:

- Determining security gaps and identifying transportation security priorities;
- Developing security, response, and recovery plans to protect public transportation assets; and
- Collaborating with 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 owners and operators to take specific actions to provide for passenger and commodity safety and security. In addition, owners and 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;
- Exercising security plans;
- Establishing continuity plans and programs that sustain critical transportation functions during a security-related incident;
- Participating in coordination bodies, information sharing groups, and mechanisms such as the Sector Coordinating Councils, Information Sharing and Analysis Centers (ISACs), 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; and
- Reporting physical and cybersecurity and safety incidents.

Industry associations represent many owners and operators in collaborative forums with federal and SLTT government entities. For example, the Sector Coordinating Council, chartered under the Critical Infrastructure Partnership Advisory Council (CIPAC), facilitates quick consultation and advice from industry to the government. [38]

The Surface Transportation Security Advisory Committee (STSAC) was established in July 2019 under the Federal Aviation Administration (FAA) Reauthorization Act of 2018 (Public Law 115-254, 132 Stat. 3186, October 5, 2018). The STSAC serves 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.

[38] https://www.dhs.gov/transportation-sector-charters-and-membership.

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.[39]

The STSAC focuses 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

In addition to enforcing applicable regulatory requirements, 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 and passenger rail Baseline Assessment for Security Enhancement (BASE), and highway and 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." [40] The report describes the process and products available for

[39] https://www.tsa.gov/for-industry/surface-transportation-security.

[40] 49 U.S.C. §114(u)3.

sharing pertinent threat and incident information, recommended practices, protective measures, and domain awareness updates with stakeholders.

TSA I&A developed the Surface Information Sharing Cell (SISC) to expand information sharing with surface stakeholders, including unclassified and classified finished threat intelligence. The SISC partnered with industry and government stakeholders on the STSAC and the sector and government coordinating councils to approve and sign the joint industry-government charter in October 2022. TSA I&A expects SISC to reach full operational capability after permanent resources are in place.

Additionally, TSA disseminates Security Awareness Messages (SAM) and Cybersecurity Awareness Messages (CAM), 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 during peak periods of travel and mass congregation such as Memorial Day and Independence Day.

TSA also works with the Surface Transportation ISACs including the Public Transportation (PT), Over-the Road Bus (OTRB), Oil and Natural Gas (ONG), and Downstream Natural Gas (DNG) ISACs to share information on threats, vulnerabilities, and solutions to physical and cyber infrastructure. In addition to serving as a clearinghouse for information on threats, the ISACs also provide updates in the event of actual security threats or attacks against the transportation systems sector.

TSA also conducts monthly, quarterly, and ad-hoc teleconferences that provide threat and intelligence updates to law enforcement and security leads for mode-specific transportation. Additionally, TSA conducts more thorough in-person consultations and coordination with officials from CISA, FBI, DHS, FEMA, DOE, 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 also supports the American Public Transportation Association in running the Public Transportation-Information Sharing and Analysis Center. This center provides 24/7 information sharing across the surface transportation community to include threats, situational awareness and other relevant information.

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. TSA field intelligence officers and headquarters personnel deliver in-person intelligence briefings, both unclassified and classified, to share critical security information about evolving and expanding threats to surface transportation.

Evolving Threats and Technology

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. While the use of UAS by terrorists is not a new tactic, the exponential proliferation of UAS and their demonstrated use to attack critical infrastructure overseas—as recently as August 2021, a bomb-laden drone crashed into an airport in southwestern Saudi Arabia, wounding eight people and damaging a civilian plane—raise the concern of such an attack or disruption domestically.[41] Terrorists continue to develop and deploy innovative concealment methods, like using laptops to conceal explosives. Although domestic incidents of chemical, biological, radiological, or nuclear attacks have been few, these threats also present a significant future risk due to the growing accessibility of the underlying technologies associated with the use of these agents as weapons.

Further, in March 2022, Yemen's Houthi rebels launched multiple cross-border attacks. No casualties were reported[42] but the incident resulted in a temporary reduction of oil output at an energy facility, according to Saudi officials.[43]

[41] FAA Information Note, Yemen Conflict: Suspected Houthi Attacks in Yemen and Saudi Arabia, 31 August 2021.
[42] FAA Information Note, Saudi Arabia/Yemen: Houthi UAS Attack in Riyadh, 17 March 2022.
[43] https://www.timesofisrael.com/houthi-drone-attack-causes-temporary-reduction-in-saudi-oil-output/.

Mass Transit and Passenger Rail Security Strategic Plan

I. Introduction

A. Overview

Public transportation[44] 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) there were nearly 10 billion public transportation unlinked trips in 2019.[45] Americans board public transportation 34 million times each weekday.[46] 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.

In calendar years 2020 and 2021, ridership numbers were significantly affected by the COVID-19 pandemic for our Mass Transit and Passenger Rail partners. In 2021, ridership was approximately 4.8 billion trips.[47]

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.[48, 49]

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.

[44] "Public transportation" means the transportation of passengers whether or not for hire by any means of conveyance, including but not limited to a street railway, elevated railway or guideway, subway, motor vehicle or motor bus, either publicly or privately owned and operated, holding itself out to the general public for the transportation of persons.
[45] https://www.apta.com/news-publications/public-transportation-facts/.
[46] https://www.apta.com/news-publications/public-transportation-facts/.
[47] https://www.apta.com/research-technical-resources/transit-statistics/ridership-report/ridership-report-archives/.
[48] 49 U.S.C. § 114(s).
[49] 6 U.S.C. § 1133.

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 owner/operator compliance with industry standards, accurate and timely exchange of intelligence and information, facilitating security drills and exercises, and publishing regulations and security directives as appropriate.

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, supporting random baggage screening, and conducting drills and exercises with transit partners through the Intermodal Security Training and Exercise Program. Further, considering the growing cybersecurity threat, TSA works with our industry partners to conduct cybersecurity workshops to discuss the cybersecurity threat and provide best practices. 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.

In fiscal year (FY) 2020, Amtrak service and ridership was significantly impacted by the COVID-19 pandemic. FY 2020 ridership decreased by 48 percent (to 16.8 million trips) compared to FY 2019. Ridership on the Northeast Corridor decreased by 51 percent of 6.1 million trips during that time frame. In FY 21 ridership remained impacted by the COVID -19 pandemic with Amtrak reporting roughly 12.2 million trips taken. Ridership on the Northeast

Corridor decreased to 4.4 million trips.[50] 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.[51] Freight railroads own and control 72 percent of the track on which Amtrak operates.[52]

Rail passenger transportation services are provided by multiple commuter railroads operating in metropolitan areas. Dozens of the commuter railroads operate 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.

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 the open nature of the infrastructure also makes certain security measures, such as airport-style checkpoints impractical. Other methods and technologies—such as the presence of visible law enforcement and/or other security personnel, 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 points.

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 U.S. 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

[50] https://www.amtrak.com/content/dam/projects/dotcom/english/public/documents/corporate/nationalfactsheets/Amtrak-Company-Profile-FY2021-030922.pdf.
[51] https://www.apta.com/wp-content/uploads/APTA_Fact-Book-2019_FINAL.pdf. Accessed June 10, 2019.
[52] https://www.amtrak.com/national-facts. Accessed May 11, 2017.

complex attacks using VBIEDs to attacks by lone offenders using edged weapons. Unsophisticated tactics and techniques terrorists used overseas could easily be used to conduct similar attacks in the United States.

Further, cybersecurity incidents affecting surface transportation are a growing threat. Malicious cyber actors continue to target U.S. critical infrastructure, to include freight, passenger and rail transit systems, with multiple cyber-attack and cyber espionage campaigns. Recent ransomware attacks against this sector underscores this threat. The U.S. adversaries and strategic competitors will continue to use cyber espionage and cyber-attacks to seek political, economic, and military advantage over the United States and its allies and partners.

3) Risk Scenarios and Security Assessments

Public transportation and 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, not listed in any particular order, include:

- Armed assault and active-shooter situations,
- Cyber-attack to IT and OT networks and systems,
- 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 U.S."),[53]
- Chemical/biological attacks,
- Sabotage of infrastructure causing derailment, and
- Vehicle ramming

Operationally, the risk scenarios inform the selection of activities used to implement risk-based priorities and address security vulnerabilities.[54] Along with physical threats, cyber threats that could disrupt operations or affect safe operation of transit systems and are a growing concern.

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 (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

[53] https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat.
[54] Transportation Sector Security Risk Assessment 8.0 (2021).

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 corporate security posture of public transportation systems in the operating environment is TSA's 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 current FY 2020/2021 TSSRA version includes the risk scenario—vehicle ramming attack on pedestrian concentrations in areas with adjacent, open-access roadways.

B. Threat Analysis

TSA issues modal threat assessments annually as well as specific and recurring analyses of threats or violent extremist messaging that provides context on the terrorism threat to the United States, the Transportation Sector, mass transit systems, and passenger railroads. These assessments analyze key terrorist actors' and groups' intent and capabilities to attack mass transit and passenger rail systems. They include information on recent attacks, modes of attack, and other tactics, techniques, and procedures which provide a threat level based on this analysis. Operationally, these assessments help federal, state, and local government security officials and industry professionals protect mass transit systems and passenger railroads from attacks.

C. Other Actions

Transit Security Grant Program

Security Grant Programs, including the Transit Security Grant Program and the Intercity Passenger Rail Security Grant Program (Amtrak), authorized by 6 U.S.C § 1152 and § 1164 respectively, are administered by FEMA in collaboration with TSA. These programs directly support physical and cyber security activities for public transportation operational and capital infrastructure.

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). These investments 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 and Directives

As part of the 9/11 Act,[55] Congress mandated regulations to enhance surface transportation security through security training of frontline employees. The mandate includes prescriptive requirements for who must be trained, what the training must encompass, and how to submit and obtain approval for a security training program.[56] The 9/11 Act also mandates regulations requiring higher-risk railroads and over-the-road buses (OTRBs) to appoint security coordinators.[57] By issuing this Security Training Rule, TSA fulfilled important elements of its transportation security mission in partnership with its industry and government stakeholders.

Concurrent with the issuance of the Security Training Rule, TSA expanded the requirements for security coordinators/alternate security coordinators and reporting of significant security concerns (which had been limited to rail operations) to include bus operations within the scope of the security training regulation's applicability.[58] In life-threatening circumstances or any actual event, owners/operators and/or their employees should first notify and work with first responders. After immediate security and safety concerns have been addressed, the TSA Transportation Security Operations Center (TSOC) should be contacted to ensure effective communication regarding threats (both to regulated parties and from regulated parties).

Notably, TSA expanded the applicability of security coordinator and security reporting requirements to include owner/operators of higher risk bus.[59] The regulatory deadline for security coordinator notification to TSA was October 28, 2020. The intent of the security reporting measures is to enhance TSA's ability to recognize potential security trends Nation-wide and to communicate directly with designated points of contacts within higher-risk operations that have direct responsibility for security.

The security training program requirement addresses who must be trained, what the training must encompass, and how to submit and obtain TSA approval for a security training program. The regulatory intent is to train surface transportation security-sensitive employees[60] to observe and assess security threats (such as a suspected improvised explosive device, suspicious behavior, security breaches, or tampering to infrastructure) and prepare them to respond to and report terrorist-related threats and/or incidents.[61]

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

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

[57] *See* sections 1512 and 1531 of the 9/11 Act, codified at 6 U.S.C. 1162 and 1181, respectively.

[58] *See* 49 CFR 1570.201 and 1570.203.

[59] Sections 1512 and 1531 of the 9/11 Act.

[60] Security-sensitive employees include any direct employee, contractor, employee of a contractor, or other authorized person who is compensated for performing a security-sensitive job function, on behalf of or for the benefit of an owner or operator.

[61] https://www.tsa.gov/for-industry/surface-security-training-rule.

On March 23, 2020, TSA published the Security Training for Surface Transportation Employees Final Rule in the Federal Register.[62] In special consideration of ongoing challenges to the surface transportation industry due to COVID-19, TSA took the following actions:

- On May 1, 2020, TSA delayed the effective date of the final rule to September 21, 2020, for owners/operators required to comply with the regulation.[63]

- On October 26, 2020, TSA extended the compliance deadline[64] for submitting security training programs from December 21, 2020, to March 22, 2021.[65]

- TSA issued its third final rule amendment on May 4, 2021,[66] extending the security training program submission deadline to June 21, 2021, in response to industry request for an additional extension, due to COVID-19 and TSA's issuance of the Mask Security Directive on January 31, 2021. (Many of the regulated entities subject to the rule were also subject to the mask requirements.[67])

These three amendments provided a total of 274 days of additional time for submitting security training programs.[68]

Upon TSA review and approval of the security training program, owner/operators must take the following actions:

- Provide security training to new employees within 60 days from first performing security-sensitive functions.[69]
- Provide initial training of security-sensitive employees within 1 year of plan approval by TSA (or 15 months if the program was submitted for approval on or before March 22, 2021).[70]

[62] Published at 85 FR 16456 (March 23, 2020). TSA initially scheduled the final rule to take effect on June 22, 2020, with the first compliance deadline set for July 22, 2020.

[63] Published at 85 FR 25315 (May 1, 2020).

[64] 49 CFR 1570.109(b)(1) and (b)(2).

[65] Published at 85 FR 67681 (October 26, 2020).

[66] Extensions published at 85 FR 25315 (May 1, 2020); 85 FR 67681 (October 26, 2020).

[67] These requirements include Executive Order (E.O.) 13998 of January 21, 2021, (Promoting COVID-19 Safety in Domestic and International Travel), as further directed and implemented pursuant to the Secretary of Homeland Security's January 27, 2021, Determination of a National Emergency (Requiring Actions to Protect the Safety of Americans Using and Employed by the Transportation System), Centers for Disease Control and Prevention's Order, TSA's security directive issued under the authority of 49 U.S.C. 114, and additional actions taken by the operating administrations of the Department of Transportation (DOT). *See,* Emergency Order No. 32, Notice No.1, of the Federal Railroad Administration, Emergency Order Requiring Face Mask Use in Railroad Operations (dated Feb. 24, 2021), available at https://railroads.dot.gov/sites/fra.dot.gov/files/2021-03/2021-04233.pdf.

[68] For owners/operators that submitted a training program for approval by the March 22, 2021 deadline, TSA revised 49 CFR 1570.111(a) to ensure that the time extension did not disadvantage these owners/operators who submitted their programs, but may still be addressing the operational issues related to COVID-19 that may make it difficult to comply with the security training requirements.

[69] 49 CFR 1570.111(a)(3).

[70] 49 CFR 1570.111(a)(1) and (2).

- Conduct recurrent training of security-sensitive employees within 3 years of initial training.[71]

Additionally, the 9/11 Act requires public transportation agencies at high risk for terrorism, as determined by the Secretary of Homeland Security, to conduct vulnerability assessments and develop comprehensive security plans. TSA is developing regulations to implement these mandates.[72]

On December 1, 2021, TSA issued Security Directive (1582-21-01)[73] "Enhancing Public Transportation and Passenger Railroad Cybersecurity" due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure. This security directive (SD) is regulatory in nature and affected passenger railroad systems must take appropriate actions.[74] In addition, TSA issued an Information Circular Enhancing Surface Transportation Cybersecurity to the broader public transportation and passenger railroad community.[75] The information circular (IC), while not regulatory, recommends agencies take four actions to help secure critical systems.

The SD and IC are designed to help prevent significant harm to the national and economic security of the United States that could result from damage to the systems that control this infrastructure. They were issued following consultation with industry and government partners after the Secretary's 60-day Cybersecurity Transportation Sprint, which concluded in October 2021.[76]

The directive required four actions:

- Designate a Cybersecurity Coordinator,
- Report cybersecurity incidents to CISA within 24 hours,
- Develop and implement a cybersecurity incident response plan, and
- Complete a cybersecurity vulnerability assessment to benchmark against applicable standards.

More recently, based upon this emerging threat, TSA recommended additional actions in IC, 2022-01, issued on February 25, 2022. It recommends that public transportation and passenger rail review, and as appropriate, implement recommendations in the Joint Cybersecurity Alert, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, January 11, 2022, as well as those identified on CISA's website under "Shields Up."

[71] 49 CFR 1570.111(b)(1).

[72] As required by section 1405 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. 110-53 (August 3, 2007). Surface Transportation Vulnerability Assessments and Security Plans (VASP) Advance Notice of Proposed Rulemaking (ANPRM) published 12/16/2016 (81 FR 91401); (82 FR 13575) https://www.tsa.gov/sites/default/files/report_on_tsa_rulemakings.pdf.

[73] https://www.tsa.gov/sites/default/files/sd-1582-21-01_signed.pdf.

[74] 49 U.S.C. 114(l)(2).

[75] https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf.

[76] https://www.dhs.gov/topics/cybersecurity.

TSA subsequently issued Security Directive (SD) 1580/82-2022-01, Rail Cybersecurity Mitigation Actions and Testing, to respond to the ongoing cybersecurity threat to railroads. The SD was effective on October 24, 2022. The SD requires that TSA-specified passenger and freight railroad owner/operators take action to prevent disruption and degradation to their infrastructure to achieve the following critical security outcomes. They must implement network segmentation policies and controls to ensure that the Operational Technology (OT) system can continue to safely operate in the event that an Information Technology (IT) system has been compromised. They must implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems. They must ensure continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations, and they must reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems in a timely manner using a risk-based methodology.

This SD also requires designated rail owners/operators to establish and execute a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures the passenger and freight rail owner/operators will utilize to achieve the security outcomes set forth in the security directive. After the Cybersecurity Implementation Plans are approved by TSA, the designated owner/operator must establish a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve vulnerabilities within devices, networks, and systems.

The applicability of this SD differs from the SDs issued to rail Owner/Operators in 2021, based upon consultation with the Department of Defense (DOD) and emerging information regarding cybersecurity threats. This expanded applicability includes railroads that operate on Strategic Rail Corridor Network (STRACNET), including those that are either the “first mile” carrier for DOD shipments to the Nation’s rail network, the “last mile” carrier to a port of departure, or operate a significant section – greater than 100 miles.

In parallel with issuance of new SD 1580/82-2022-01, TSA also revised the previously issued SDs applicable to railroads. First, the amendments expanded the applicability of the SD 1580-21-01 series to align with the applicability of SD 1580/82-2022-01. This expanded applicability includes railroads that support the STRACNET. Second, TSA extended the expiration dates of these SDs from December 31, 2022, to October 24, 2023. Third, the SDs issued to rail Owner/Operators in 2021 included a requirement to develop a Cybersecurity Incident Response Plan by a certain date. While that date had passed prior to the amendment, it is critical that rail Owner/Operators maintain and regularly update their Cybersecurity Incident Response Plans. To address this concern, the amendments made the response plans an ongoing requirement for those currently subject to the SDs.

II. Objectives, Activities, and Measuring Progress

The MTPR goals and objectives reflect the risk-based priorities. Figure 9 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 9: Mass Transit and Passenger Rail Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.1: Security Planning 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).	**Activity 1.1.1:** Develop, review, and update security plans based on available information. (Industry/DHS/TSA) **Outcome:** Improvement of industry security plans and security planning for both physical and cybersecurity through incorporation of best practices and lessons learned. **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) --- **Activity 1.1.2:** Develop a comprehensive cybersecurity risk management program. (Industry/DHS/TSA) **Outcome:** Improvement of MTPR cybersecurity practices through incorporation of comprehensive cybersecurity risk management program. **Performance Measure:** Percentage of high-risk MTPR operators that have implemented a comprehensive risk management program. (Industry/DHS/TSA) -- **Activity 1.1.3**: For TSA-identified critical owner/operators, develop and implement a cybersecurity incident response plan as required by TSA Security Directive/1582-21-01. (Industry/DHS/TSA) **Outcome**: Comprehensive and up-to-date cybersecurity incident response plans that reduce risk by explicitly addressing transit and rail cybersecurity policies and procedures. **Performance Measurement**: Percentage of regulated parties whose cybersecurity incident response plans are compliant with the requirements in the TSA Security Directives as assessed through compliance verification/inspections. (DHS/TSA) -- **Activity 1.1.4:** For applicable MTPR owners/operators implement recommendations from the TSA Information Circular IC-2021-01. (Industry/DHS/TSA) **Outcome:** Enhance sector resiliency by having comprehensive and up-to-date cybersecurity incident response plans that reduce risk by explicitly addressing MTPR policies and procedures.

	Performance Measurement: Number of MTPR operators that have voluntarily appointed a Cybersecurity Coordinator to TSA in accordance with the Information Circular (Surface Transportation IC-2021-01). (Industry/DHS/TSA) Number of MTPR operators that have attested to the development and implementation of a cybersecurity incident response plan in accordance with the IC. (Industry/DHS/TSA)
Objective 1.2: Security Training Conduct training of employees to identify, prevent, respond, and recover from a terrorist attack.	**Activity 1.2.1:** For regulated entities, train all security-sensitive employees within the timeframe specified in the regulation. (Industry/DHS/TSA) **Outcome:** Improve capability of security-sensitive industry employees to observe, assess and report suspicious activities. **Performance Measurement:** Percentage of regulated higher-risk transit and passenger rail entities that are in compliance with the requirements of the training rule as assessed through compliance verification/inspections. (Industry/DHS/TSA)
Objective 1.3: Security Exercises Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.	**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) **Outcome:** MTPR systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents. **Performance Measurement:** Percentage of higher-risk transit agencies assessed during the measurement period that achieved a positive rating for security exercises, including TSA's Intermodal Security Training and Exercise Program exercises, using the BASE. (DHS/TSA)

NSTS Goa1 2	**Enhance effective domain awareness of transportation systems and threats**
Objective 2.1: Intelligence and Information Sharing Maintain and enhance mechanisms for information and intelligence sharing between the MTPR industry and government.	**Activity 2.1.1:** Provide timely and relevant information and intelligence to enhance industry's domain awareness. (DHS/TSA) **Outcome:** Sustain domain awareness through timely delivery of relevant intelligence and information products for MTPR industry to implement mitigation strategies to reduce risk. **Performance Measurement:** Percentage of intelligence products delivered to MTPR stakeholders within 24 hours of release. (DHS/TSA)
Objective 2.2: Community Outreach Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with MTPR systems.	**Activity 2.2.1:** Promote MTPR security awareness in communities surrounding critical MTPR assets and systems. (DHS/TSA) **Outcome:** MTPR industry, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt MTPR operations and endanger the community. **Performance Measurement:** Percentage of higher-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)

III. MTPR Operational Recovery Plan

Transportation modal security plans should include an operational recovery plan to expedite the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident.[77]

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.[78] 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.

[77] 49 U.S.C § 114(s).

[78] https://www.transportation.gov/disaster-recovery.

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.[79] 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.[80,81] Effective coordination and integration of all entities contributing to disaster response and recovery are necessary for quick recovery of essential public transportation services.

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

[80] https://www.transportation.gov/tags/disaster-recovery.

[81] https://www.transportation.gov/emergency.

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.[82,83]

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 of reported incidents from regulated stakeholders and communication of threat information to all transportation stakeholders;
- Establishment of risk-based priorities to ensure appropriate resourcing and administration of security measures; and
- 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 140,000 rail miles operated by seven Class I

[82] 49 U.S.C. § 114(s).
[83] 6 U.S.C. § 1161.

railroads—railroads with operating revenues of $505 million or more, 21 regional railroads, and 580 local (also known as Short Line) railroads. The Class I railroads account for approximately 68 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.[84]

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 FRA. TSA administers and enforces rail security regulations contained in 49 CFR Parts 1570 and 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 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)[85] shipments through densely populated areas and High Threat Urban Areas (HTUAs) and cyber risks to

[84] https://www.aar.org/wp-content/uploads/2020/08/AAR-Railroad-101-Freight-Railroads-Fact-Sheet.pdf.
[85] 49 CFR § 1580.3.

freight rail operations that could adversely affect critical supply chains of food, fuel, and other raw materials essential for critical industries.

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.[86,87]

- 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 (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 U.S.");[88] and
- Cyber-attack on IT or OT equipment or infrastructure.

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

[86] Transportation Sector Security Risk Assessment 8.0 (2021).
[87] 2021 Freight Rail Modal Threat Assessment (TSA Office of Intelligence and Analysis).
[88] https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat.

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.

B. Threat Analysis

TSA issues modal threat assessments 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 rail. These products describe key terrorist actors and group ideologies, recent attacks, modes of attack, and other tactics, techniques, and procedures used by threat actors (including foreign terrorist organizations, HVEs, and domestic violent extremists) and provide a threat level based on these analyses. Operationally, these assessments help federal, state, and local government security officials and industry professionals protect U.S. railroads from attacks.

C. Other Actions

Security Regulations and Directives

As part of the 9/11 Act,[89] Congress mandated regulations to enhance surface transportation security through security training of frontline employees. The mandate includes prescriptive requirements for who must be trained, what the training must encompass, and how to submit and obtain approval for a security training program.[90] The 9/11 Act also mandates regulations requiring higher-risk railroads and over-the-road buses (OTRBs) to appoint security coordinators.[91] By issuing this Security Training Rule, TSA fulfilled our transportation security mission in partnership with its industry and government stakeholders.

The Security Training Rule requires regulated entities to designate primary and alternate security coordinators and to report actual and suspected security threats to TSA within 24 hours of the initial discovery of the incident.[92] In life-threatening circumstances or any actual event, owners/operators and/or their employees should first notify and work with first responders. After immediate security and safety concerns have been addressed, the TSA TSOC should be contacted to ensure effective communication regarding threats (both to regulated parties and from regulated parties).

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

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

[91] *See* sections 1512 and 1531 of the 9/11 Act, codified at 6 U.S.C. 1162 and 1181, respectively.

[92] 49 CFR 1570.203.

Notably, TSA expanded the applicability of existing security coordinator and security reporting requirements for operations to include owner/operators of higher risk bus.[93] The regulatory deadline for security coordinator notification to TSA was October 28, 2020. The intent of the security reporting measures is to enhance TSA's ability to recognize potential security trends Nation-wide and to communicate directly with designated points of contacts within higher-risk operations that have direct responsibility for security.

The security training program mandate includes prescriptive requirements for who must be trained, what the training must encompass, and how to submit and obtain TSA approval for a security training program. The regulatory intent is to train surface transportation security-sensitive employees[94] to observe and assess security threats (such as a suspected IEDs, suspicious behavior, security breaches, or tampering to infrastructure) and prepare them to respond to and report terrorist-related threats and/or incidents.[95]

On March 23, 2020, TSA published the Security Training for Surface Transportation Employees Final Rule in the Federal Register.[96] In special consideration of ongoing challenges to the surface transportation industry in response to COVID-19, on May 1, 2020, TSA delayed the effective date of the final rule to September 21, 2020, due to strain on resources for owners/operators required to comply with the regulation.[97] On October 26, 2020, TSA extended the compliance deadline[98] for submitting security training programs from December 21, 2020, to March 22, 2021.[99]

Industry requested an additional extension of the security training program submission date, due to ongoing COVID-19 impacts and TSA's issuance of the Mask Security Directive on January 31, 2021; many of the regulated entities subject to the rule were also subject to the mask requirements.[100] In response, TSA issued its third final rule amendment on May 4, 2021,[101]

[93] Sections 1512 and 1531 of the 9/11 Act.

[94] Security-sensitive employees include any direct employee, contractor, employee of a contractor, or other authorized person who is compensated for performing a security-sensitive job function, on behalf of or for the benefit of an owner or operator.

[95] https://www.tsa.gov/for-industry/surface-security-training-rule.

[96] Published at 85 FR 16456 (March 23, 2020). TSA initially scheduled the final rule to take effect on June 22, 2020, with the first compliance deadline set for July 22, 2020.

[97] Published at 85 FR 25315 (May 1, 2020).

[98] 49 CFR 1570.109(b)(1) and (b)(2).

[99] Published at 85 FR 67681 (October 26, 2020). TSA initially scheduled the final rule to take effect on June 22, 2020, with the first compliance deadline set for July 22, 2020.

[100] These requirements include Executive Order (E.O.) 13998 of January 21, 2021, (Promoting COVID-19 Safety in Domestic and International Travel), as further directed and implemented pursuant to the Secretary of Homeland Security's January 27, 2021, Determination of a National Emergency (Requiring Actions to Protect the Safety of Americans Using and Employed by the Transportation System), Centers for Disease Control and Prevention's Order, TSA's security directive issued under the authority of 49 U.S.C. 114, and additional actions taken by the operating administrations of the Department of Transportation (DOT). *See,* Emergency Order No. 32, Notice No.1, of the Federal Railroad Administration, Emergency Order Requiring Face Mask Use in Railroad Operations (dated Feb. 24, 2021), available at https://railroads.dot.gov/sites/fra.dot.gov/files/2021-03/2021-04233.pdf.

[101] Extensions published at 85 FR 25315 (May 1, 2020); 85 FR 67681 (October 26, 2020).

extending the security training program submission deadline to June 21, 2021. These three amendments provided a total of 274 days of additional time for submitting security training programs.[102]

TSA is implementing the security training rule to solidify the baseline of security for higher-risk surface transportation operations by giving frontline employees tools to observe, assess, and respond to security risks and potential security breaches within their specific working environment. Upon TSA review and security training program approval, owner/operators must provide security training to new employees within 60 days from first performing security-sensitive functions.[103] Owner/operators must provide initial training of security-sensitive employees within one year of plan approval by TSA (or 15 months if the program was submitted to TSA for approval on or before March 22, 2021).[104] Owner/operators must conduct recurrent training of security-sensitive employees within three years of initial training.[105]

Additionally, the 9/11 Act requires freight railroad owner/operators, 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.[106]

Furthermore, due to the ongoing cybersecurity threat to surface systems and associate infrastructure, on December 1, 2021, TSA issued SD (1580-21-01)[107] "Enhancing Rail Cybersecurity." This directive is regulatory in nature and systems impacted are required to take appropriate actions. In parallel to the SD, TSA issued an IC "Enhancing Surface Transportation Cybersecurity"[108] to the broader railroad community. The IC recommends owner/operators to take four actions, yet it is not regulatory in nature.

The actions required by the SD and recommended by the information circular are:

- Designate a cybersecurity coordinator;
- Report cybersecurity incidents to CISA within 24 hours;
- Develop and implement a cybersecurity incident response plan to reduce the risk of an operational disruption; and
- Complete a cybersecurity vulnerability assessment to identify potential gaps or vulnerabilities in their systems.

[102] For owners/operators that submitted a training program for approval by the March 22, 2021 deadline, TSA revised 49 CFR 1570.111(a) to ensure that the time extension did not disadvantage these owners/operators who submitted their programs, but may still be addressing the operational issues related to COVID-19 that may make it difficult to comply with the security training requirements.

[103] 49 CFR 1570.111(a)(3).

[104] 49 CFR 1570.111(a)(1) and (2).

[105] 49 CFR 1570.111(b)(1).

[106] As required by section 1405 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. 110-53 (August 3, 2007). Surface Transportation Vulnerability Assessments and Security Plans (VASP) Advance Notice of Proposed Rulemaking (ANPRM) published 12/16/2016 (81 FR 91401); (82 FR 13575) (81 FR 91401); (82 FR 13575) https://www.tsa.gov/sites/default/files/report_on_tsa_rulemakings.pdf.

[107] https://www.tsa.gov/sites/default/files/sd-1580-21-01_signed.pdf.

[108] https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf.

On February 25, 2022, based upon the emerging threat, TSA issued additional guidance recommending actions in addition to those previously recommended through the December 2021 guidance. Information Circular 2022-01, recommends that freight rail owner/operators review, and as appropriate, implement recommendations in the Joint Cybersecurity Alert, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, January 11, 2022, as well as those identified on CISA's website under "Shields Up."

TSA subsequently issued Security Directive (SD) 1580/82-2022-01, *Rail Cybersecurity Mitigation Actions and Testing*, to respond to the ongoing cybersecurity threat to railroads. The SD was effective on October 24, 2022. The SD requires that TSA-specified passenger and freight railroad owner/operators take action to prevent disruption and degradation to their infrastructure to achieve the following critical security outcomes. They must implement network segmentation policies and controls to ensure that the Operational Technology (OT) system can continue to safely operate in the event that an Information Technology (IT) system has been compromised. They must implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems. They must ensure continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations, and they must reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems in a timely manner using a risk-based methodology.

This SD also requires designated rail owners/operators to establish and execute a TSA-approved Cybersecurity Implementation Plan that describes the specific cybersecurity measures the passenger and freight rail owner/operators will utilize to achieve the security outcomes set forth in the security directive. After the Cybersecurity Implementation Plans are approved by TSA, the designated owner/operator must establish a Cybersecurity Assessment Program to proactively test and regularly audit the effectiveness of cybersecurity measures and identify and resolve vulnerabilities within devices, networks, and systems.

The applicability of this SD differs from the SDs issued to rail Owner/Operators in 2021, based upon consultation with the Department of Defense (DOD) and emerging information regarding cybersecurity threats. This expanded applicability includes railroads that operate on Strategic Rail Corridor Network (STRACNET), including those that are either the "first mile" carrier for DOD shipments to the Nation's rail network, the "last mile" carrier to a port of departure, or operate a significant section – greater than 100 miles.

In parallel with issuance of new SD 1580/82-2022-01, TSA also revised the previously issued SDs applicable to railroads. First, the amendments expanded the applicability of the SD 1580-21-01 series to align with the applicability of SD 1580/82-2022-01. This expanded applicability includes railroads that support the STRACNET. Second, TSA extended the expiration dates of these SDs from December 31, 2022, to October 24, 2023. Third, the SDs issued to rail Owner/Operators in 2021 included a requirement to develop a Cybersecurity Incident Response Plan by a certain date. While that date had passed prior to the amendment, it is critical that rail Owner/Operators maintain and regularly update their Cybersecurity Incident Response Plans. To address this concern, the amendments made the response plans an ongoing requirement for those currently subject to the SDs.

The Hazardous Materials Regulations (49 Code of Federal Regulations Part 172), which are issued by DOT's 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.

II. Objectives, Activities, and Measuring Progress

The Freight Rail Security Plan's goals and objectives reflect the risk-based priorities. **Figure 10** highlights the path forward to address unique modal challenges identified in the risk profile and the corresponding activities that encompass the whole-of-government approach to national 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 10: Freight Rail Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.1: **Security Planning** 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).	**Activity 1.1.1:** Develop, review, and update security plans based on available information. (Industry/DHS/TSA) **Outcome:** Improvement of railroad security plans and security planning for both physical and cybersecurity through incorporation of best practices and lessons learned into existing security plans. **Performance Measurement:** Percentage of railroads that transport RSSM in HTUAs with implemented security plans. (DHS/TSA)
	Activity 1.1.2: Develop a comprehensive cybersecurity risk management program. (Industry/DHS/TSA) **Outcome:** Improvement of railroad cybersecurity practices through incorporation of comprehensive cybersecurity risk management program. **Performance Measurement:** Percentage of higher-risk railroads that have implemented a comprehensive risk management program. (Industry/DHS/TSA)
	Activity 1.1.3: For TSA identified critical owner/operators, develop and implement a cybersecurity incident response plan as required by TSA Security Directive/1580-21-01. (Industry/DHS/TSA) **Outcome:** Comprehensive and up-to-date cybersecurity incident response plans that reduce risk by explicitly addressing freight rail cybersecurity policies and procedures. **Performance Measurement:** Percentage of regulated parties whose cybersecurity incident response plans are compliant with the requirements in the TSA Security Directive as assessed through compliance verification/inspections.
	Activity 1.1.4: For applicable railroad owners/operators, implement recommendations from the TSA Information Circular IC-2021-01**.** **Outcome:** Enhance sector resiliency by having comprehensive and up-to-date cybersecurity incident response plans that reduce risk by explicitly addressing railroad policies and procedures. **Performance Measurement:** Number of railroad operators that have appointed a Cybersecurity Coordinator to TSA in accordance with the Information Circular (Surface Transportation IC-2021-01). Number of railroad operators that have attested to the development and implementation of a cybersecurity incident response plan in accordance with the Information Circular (Surface Transportation IC-2021-01).

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.2: **Security Training** Conduct training of frontline employees to identify, prevent, and respond to a terrorist attack.	**Activity 1.2.1:** For regulated entities under 49 CFR 1580.113, train all security-sensitive employees within the timeframe specified in the regulation. **Outcome:** Security-sensitive employees are properly trained to prepare, observe, and respond to security incidents. **Performance Measure:** Percentage of regulated railroads that are in compliance with the requirements of the training rule as assessed through compliance verification/inspections. (Industry/DHS/TSA)
Objective 1.3: **Security Exercises** Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.	**Activity 1.3.1:** Railroads participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents. (Industry/DOT/DHS/TSA) **Outcome:** Railroads and public safety agencies are better prepared to respond and recover effectively in the event of physical and cybersecurity incidents. **Performance Measurement:** Percentage of RSSM railroads in HTUAs that conducted or participated in security-related exercises. (DHS/TSA)

NSTS Goal 2	**Enhance effective domain awareness of transportation systems and threats**
Objective 2.1: **Intelligence and Information Sharing** Maintain and enhance mechanisms for information and intelligence sharing between the freight rail industry and government.	**Activity 2.1.1:** Provide timely and relevant information and intelligence to enhance freight railroads' domain awareness. (DHS/TSA) **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. **Performance Measurement:** Percentage of intelligence products delivered to freight rail stakeholders within 24 hours of release. (DHS/TSA)
Objective 2.2: **Community Outreach** Engage with first responders and the public to provide awareness of security concerns associated with railroad operations to promote situational security awareness and preparedness.	**Activity 2.2.1:** Promote freight railroad security awareness in communities surrounding critical freight assets and systems. (DHS/TSA) **Outcome:** Freight railroads, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt freight operations and endanger the community. **Performance Measurement:** Railroads that transport RSSM in HTUAs report the number of engagements or activities related to enhancing the security preparedness with public safety, law enforcement, or emergency management organizations. (DHS/TSA)

III. Freight Rail Operational Recovery Plan

Transportation modal security plans should include an operational recovery plan to expedite the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident.[109]

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*.[110,111,112] 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.[113,114]

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.

[109] 49 U.S.C § 114(s).

[110] https://www.transportation.gov/disaster-recovery. Accessed May 30, 2019.

[111] https://www.transportation.gov/policy-initiatives/disaster-recovery/recovering-disasters-national-transportation-recovery-strategy. Accessed October 9, 2019.

[112] https://www.transportation.gov/emergency/usdot-recovery-resource-guide. Accessed October 9, 2019.

[113] https://www.fema.gov/national-preparedness-system. Accessed May 30, 2019.

[114] https://www.fema.gov/national-planning-frameworks. Accessed May 30, 2019.

Highway and Motor Carrier Security Plan

I. Introduction

A. Overview

The Highway and Motor Carrier (HMC) Security Plan establishes risk-based priorities to protect the Nation's roads, bridges, tunnels, cargo carriers, and OTRB 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.[115]

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, 574.6 million passenger trips occurred on OTRB and motor coaches, and more than 25 million schoolchildren rode more than 480,000 school buses each day.[116,117] 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 commerce safely and securely. Bridges, causeways, and underground and underwater tunnels are important infrastructure connections in highway systems requiring special security considerations. While

[115] 49 U.S.C. § 114(s).

[116] 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.

[117] American School Bus Council (http://www.americanschoolbuscouncil.org/about/).

the Nation's highways are resilient, large-scale disruptions of these systems may adversely affect the Nation's economy and global markets. Terrorists may attack highway assets—structures, trucks, or buses—directly or use vehicles to deploy explosives or other weapons to attack targets. 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.[118,119] These attack scenarios include but are not limited to:

- 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 (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 U.S.");[120]
- Intentional contamination of food products during bulk transportation; and
- Cyber-attack to IT and OT networks and systems.

B. Threat Analysis

TSA issues modal threat assessments 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 the highway and motor carrier sub-modes. These assessments analyze key terrorist actors and group intent and capabilities to attack highway and motor carriers, recent attacks, modes of attack, and other tactics, techniques, and procedures, provide a threat level based on this analysis. Operationally, these assessments help federal, state, and local government security officials and industry professionals protect highway transportation infrastructure and commercial vehicles moving people and commerce from attacks.

[118] Transportation Sector Security Risk Assessment 8.0 (2021).

[119] 2021 Highway and Motor Carrier Modal Threat Assessment (TSA Office of Intelligence and Analysis).

[120] https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat.

C. Other Actions

Security Regulations and Directives

As part of the 9/11 Act,[121] Congress mandated regulations to enhance surface transportation security through security training of frontline employees. The mandate includes prescriptive requirements for who must be trained, what the training must encompass, and how to submit and obtain approval for a security training program.[122] The 9/11 Act also mandates regulations requiring higher-risk railroads and over-the-road buses (OTRBs) to appoint security coordinators.[123] By issuing this Security Training Rule, TSA fulfilled our transportation security mission in partnership with its industry and government stakeholders.

The Security Training Rule requires regulated entities to designate primary and alternate security coordinators and to report actual and suspected security threats to TSA within 24 hours of the initial discovery of the incident.[124] In life-threatening circumstances or any actual event, owners/operators and/or their employees should first notify and work with first responders. After immediate security and safety concerns have been addressed, the TSA TSOC should be contacted to ensure effective communication regarding threats (both to regulated parties and from regulated parties).

Notably, TSA expanded the applicability of existing security coordinator and security reporting requirements for operations to include owner/operators of higher risk bus operations.[125] The regulatory deadline for security coordinator notification to TSA was October 28, 2020. The intent of the security reporting measures is to enhance TSA's ability to recognize potential security trends nation-wide and to communicate directly with designated points of contacts within higher-risk operations that have direct responsibility for security.

The security training program mandate includes prescriptive requirements for who must be trained, what the training must encompass, and how to submit and obtain TSA approval for a security training program. The regulatory intent is to train surface transportation security-sensitive employees[126] to observe and assess security threats (such as a suspected improvised explosive device, suspicious behavior, security breaches, or tampering to infrastructure) and prepare them to respond to and report terrorist-related threats and/or incidents.[127]

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

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

[123] *See* sections 1512 and 1531 of the 9/11 Act, codified at 6 U.S.C. 1162 and 1181, respectively.

[124] 49 CFR 1570.203.

[125] Sections 1512 and 1531 of the 9/11 Act.

[126] Security-sensitive employees include any direct employee, contractor, employee of a contractor, or other authorized person who is compensated for performing a security-sensitive job function, on behalf of or for the benefit of an owner or operator.

[127] https://www.tsa.gov/for-industry/surface-security-training-rule.

On March 23, 2020, TSA published the Security Training for Surface Transportation Employees Final Rule in the Federal Register.[128] In special consideration of ongoing challenges to the surface transportation industry in response to COVID-19, on May 1, 2020, TSA delayed the effective date of the final rule to September 21, 2020, due to strain on resources for owners/operators required to comply with the regulation.[129] On October 26, 2020, TSA extended the compliance deadline[130] for submitting security training programs from December 21, 2020, to March 22, 2021.[131]

Industry requested an additional extension of the security training program submission date, due to ongoing COVID-19 impacts and TSA's issuance of the Mask Security Directive on January 31, 2021; many of the regulated entities subject to the rule were also subject to the mask requirements.[132] In response, TSA issued its third final rule amendment on May 4, 2021,[133] extending the security training program submission deadline to June 21, 2021. These three amendments provided a total of 274 days of additional time for submitting security training programs.[134]

TSA is implementing the security training rule to solidify the baseline of security for higher-risk surface transportation operations by giving frontline employees tools to observe, assess, and respond to security risks and potential security breaches within their specific working environment. Upon TSA review and security training program approval, owner/operators must provide security training to new employees within 60 days from first performing security-sensitive functions.[135] Owner/operators must provide initial training of security-sensitive employees within one year of plan approval by TSA (or 15 months if the program was submitted to TSA for approval on or before March 22, 2021).[136] Owner/operators must conduct recurrent training of security-sensitive employees within 3 years of initial training.[137]

[128] Published at 85 FR 16456 (March 23, 2020). TSA initially scheduled the final rule to take effect on June 22, 2020, with the first compliance deadline set for July 22, 2020.
[129] Published at 85 FR 25315 (May 1, 2020).
[130] 49 CFR 1570.109(b)(1) and (b)(2).
[131] Published at 85 FR 67681 (October 26, 2020).
[132] These requirements include Executive Order (E.O.) 13998 of January 21, 2021, (Promoting COVID-19 Safety in Domestic and International Travel), as further directed and implemented pursuant to the Secretary of Homeland Security's January 27, 2021, Determination of a National Emergency (Requiring Actions to Protect the Safety of Americans Using and Employed by the Transportation System), Centers for Disease Control and Prevention's Order, TSA's security directive issued under the authority of 49 U.S.C. 114, and additional actions taken by the operating administrations of the Department of Transportation (DOT). *See,* Emergency Order No. 32, Notice No.1, of the Federal Railroad Administration, Emergency Order Requiring Face Mask Use in Railroad Operations (dated Feb. 24, 2021), available at https://railroads.dot.gov/sites/fra.dot.gov/files/2021-03/2021-04233.pdf.
[133] Extensions published at 85 FR 25315 (May 1, 2020); 85 FR 67681 (October 26, 2020).
[134] For owners/operators that submitted a training program for approval by the March 22, 2021 deadline, TSA revised 49 CFR 1570.111(a) to ensure that the time extension did not disadvantage these owners/operators who submitted their programs, but may still be addressing the operational issues related to COVID-19 that may make it difficult to comply with the security training requirements.
[135] 49 CFR 1570.111(a)(3).
[136] 49 CFR 1570.111(a)(1) and (2).
[137] 49 CFR 1570.111(b)(1).

Additionally, the 9/11 Act requires OTRB operators, 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.[138]

Further, on December 1, 2021, TSA issued an IC "Enhancing Surface Transportation Cybersecurity" to certain OTRB operators due to the ongoing cybersecurity threat to surface systems and associated infrastructure.[139] The IC recommends operators:

- Designate a Cybersecurity Coordinator,
- Report cybersecurity incidents to CISA within 24 hours,
- Develop and implement a cybersecurity incident response plan, and
- Complete a cybersecurity vulnerability assessment to benchmark against applicable standards.

These cybersecurity recommendations will help secure critical systems and prevent significant harm to the national and economic security of the United States.

More recently, based upon the emerging threat, TSA issued additional guidance recommending actions in addition to those previously recommended through the IC issued in December 2021. This IC, 2022-01, issued on February 25, 2022, recommends that OTRB operators review, and as appropriate, implement recommendations in the Joint Cybersecurity Alert, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, January 11, 2022, as well as those identified on CISA's website under "Shields Up."

The Hazardous Materials Regulations (49 Code of Federal Regulations Part 172), which are issued by DOT's 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.

Intercity Bus Security Grant Program

The Intercity Bus Security Grant Program (IBSGP) authorized by 6 U.S.C § 1182, is administered by FEMA in collaboration with TSA. This program directly supports intercity security activities for bus transportation operational and capital infrastructure.

Security grant funds are appropriated annually and awarded to eligible applicants, which include fixed-route intercity bus transportation entities providing services to Urban Area Security Initiative (UASI) regions. These investments 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.

[138] As required by section 1531 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. 110-53 (August 3, 2007). Surface Transportation Vulnerability Assessments and Security Plans (VASP) Advance Notice of Proposed Rulemaking (ANPRM) published 12/16/2016 (81 FR 91401); (82 FR 13575) https://www.tsa.gov/sites/default/files/report_on_tsa_rulemakings.pdf.

[139] https://www.tsa.gov/sites/default/files/20211201_surface-ic-2021-01.pdf.

II. Objectives, Activities, and Measuring Progress

The HMC Security Plan's 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 the whole-of-government approach to national HMC security.

Figure 11: Highway and Motor Carrier Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.1: **Security Planning** 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).	**Activity 1.1.1:** Develop, review, and update security plans based on available information. (Industry/DHS/TSA) **Outcome:** Improvement of industry security plans and security planning through incorporation of best practices and lessons learned into existing security plans. **Performance Measurement:** Percentage of motor carriers assessed during the measurement period that achieved a positive rating for security planning using the BASE. (DHS/TSA)
	Activity 1.1.2: Develop a comprehensive cybersecurity risk management program. (Industry/DHS/TSA) **Outcome:** Improvement of highway and motor carrier cybersecurity practices through incorporation of comprehensive cybersecurity risk management program. **Performance Measurement:** Percentage of higher-risk highway and motor carrier that have implemented a comprehensive risk management program. (Industry/DHS/TSA)
	Activity 1.1.3: For applicable OTRB owners/operators implement recommendations from the TSA Information Circular IC-2021-01. (Industry/DHS/TSA) **Outcome:** Enhance sector resiliency by having comprehensive and up-to-date cybersecurity incident response plans that reduce risk by explicitly addressing OTRB policies and procedures. **Performance Measurement(s):** Number of OTRB owners/operators that have appointed a Cybersecurity Coordinator to TSA in accordance with the Information Circular (Surface Transportation IC-2021-01). (Industry/DHS/TSA) Number of OTRB owners/operators that have attested to the development and implementation of a cybersecurity incident response plan in accordance with the IC. (Industry/DHS/TSA)

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.2: **Security Training** Conduct training of employees to identify, prevent, respond to and recover from a terrorist attack.	**Activity 1.2.1:** Improve the current state of the most critical OTRB owner/operator security training programs through the incorporation of best practices and lessons learned into existing training plans. (Industry/DHS/TSA) **Outcome:** Improve capability of security-sensitive industry employees to observe, assess and report suspicious activities. **Performance Measurement:** Percentage of regulated OTRB owners/operators that are in compliance with the requirements of the training rule as assessed through compliance verification inspections.
Objective 1.3: **Security Exercises** Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.	**Activity 1.3.1:** Motor carriers participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents. (Industry/DHS/TSA) **Outcome:** Motor carriers and public safety agencies are better prepared to respond and recover effectively in the event of security incidents. **Performance Measurement:** Percentage of motor carriers assessed during the measurement period that achieved a positive rating for security exercises using the BASE. (DHS/TSA)

NSTS Goal 2	**Enhance effective domain awareness of transportation systems and threats**
Objective 2.1: **Intelligence and Information Sharing** Maintain and enhance mechanisms for information and intelligence sharing between the HMC industry and government.	**Activity 2.1.1:** Provide timely and relevant information and intelligence to enhance industry's domain awareness. (DHS/TSA) **Outcome:** Sustain domain awareness through timely delivery of relevant intelligence and information products for HMC industry to implement mitigation strategies to reduce risk. **Performance Measurement:** Percentage of intelligence products delivered to HMC stakeholders within 24 hours of release by originating office. (DHS/TSA)
Objective 2.2: **Community Outreach** Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with HMC systems.	**Activity 2.2.1:** Promote HMC security awareness in communities surrounding critical HMC assets. (DHS/TSA) **Outcome:** HMC industry, first responders, and neighboring communities working collectively to plan and prepare for incidents that could disrupt HMC operations and endanger the community. **Performance Measurement:** Percentage of 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)

III. HMC Operational Recovery Plan

Transportation modal security plans should include an operational recovery plan to expedite the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident.[140]

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*.[141,142,143] 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.[144,145]

Most response and recovery actions are initiated and 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.

[140] 49 U.S.C § 114(s).

[141] https://www.transportation.gov/disaster-recovery. Accessed May 30, 2019.

[142] https://www.transportation.gov/emergency/usdot-recovery-resource-guide. Accessed October 9, 2019.

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

[144] https://www.fema.gov/national-preparedness-system. Accessed May 30, 2019.

[145] https://www.fema.gov/national-planning-frameworks. Accessed May 30, 2019.

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.

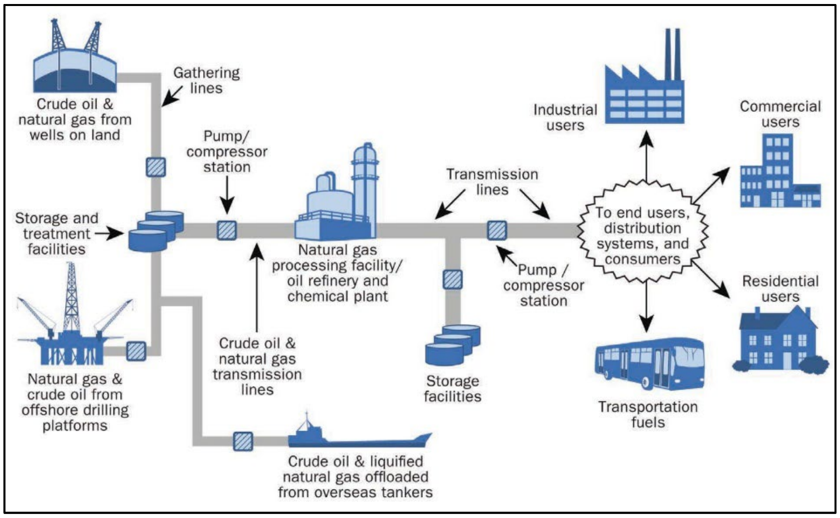
1) Modal Profile

The national pipeline system consists of more than 2.8 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 preprogramed parameters to activate valves and pumps to maintain flows within tolerances.

Pipeline systems supply energy commodities and raw materials across the country to utility entities, airports, military sites, and to the Nation's industrial and manufacturing sectors (see **Figure 12**). 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 12: The Structure of Oil and Gas Pipeline Systems Movement to Market


Crude oil & natural gas from wells on land
Gathering lines
Pump/ compressor station
Storage and treatment facilities
Natural gas processing facility/ oil refinery and chemical plant
Transmission lines
Industrial users
Commercial users
To end users, distribution systems, and consumers
Pump / compressor station
Residential users
Natural gas & crude oil from offshore drilling platforms
Crude oil & natural gas transmission lines
Storage facilities
Transportation fuels
Crude oil & liquified natural gas offloaded from overseas tankers

2) Risk Profile

The national pipeline system and associated facilities are vulnerable to terrorist and nation-state 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.

From a physical threat perspective, Animal Rights/Environmental Violent Extremists (AREVEs) and Anarchist Violent Extremists (AVEs) are the primary threat actors interested in targeting pipelines in the United States. In January 2021, a climate change activist published the book, "How to Blow Up a Pipeline" which encouraged sabotage against hazardous liquid/natural gas pipelines and discouraged pacifism in the fight against climate change. In a subsequent appearance, the activist further encouraged targeted sabotage, including the destruction or neutralization of equipment and property. These violent extremists will continue to use a variety of tactics, including criminal acts such as lower-impact sabotage and vandalism, to counter pipeline construction projects.[146]

From a cyber-threat perspective, the pipeline industry has been subject to cyber-attacks in the United States, most notably the ransomware attack against a major pipeline operator in May 2021.[147] DHS and the FBI have reported that state-sponsored advanced persistent threat actors have demonstrated the ability to maintain persistent, undetected, long-term access in compromised environments—including cloud environments—by using legitimate credentials.[148] These actors have conducted cyber operations against critical infrastructure organizations and have specifically targeted OT/ICS networks with destructive malware.

The Annual Threat Assessment of the U.S. Intelligence Community released in March 2022, by the Director of National Intelligence noted, *"China almost certainly is capable of launching cyber-attacks that would disrupt critical infrastructure services within the U.S., including against oil and gas pipelines and rail systems."*[149] Risk analysis conducted by DHS and the FBI

[146] (U/SSI) TSA Pipeline Annual Terrorism Threat Assessment – 2021.

[147] (U/SSI) TSA Cyber Targeting of Transportation in 2020: Key Actors and Trends.

[148] CISA/FBI/NSA – Joint Cybersecurity Advisory: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure, (AA22-011A, January 11, 2022).

[149] Annual Threat Assessment of the U.S. Intelligence Community, Director of National Intelligence, 7 February 2022.

in 2021 of intrusions on pipeline systems in 2011 through 2012 noted, *"The U.S. Government has attributed this activity to Chinese state-sponsored actors. CISA and the FBI assess that these actors were specifically targeting U.S. pipeline infrastructure for the purpose of holding U.S. pipeline infrastructure at risk. Additionally, CISA and the FBI assess that this activity was ultimately intended to help China develop cyber-attack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations."*[150]

3) Risk Scenarios

The following risk scenarios inform the selection of activities to implement the risk-based priorities and address security vulnerabilities.[151, 152, 153]

- AREVE 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; and
- Cyber-attacks to IT and OT networks and systems.

B. Threat Analysis

TSA issues modal threat assessments annually as well as specific and recurring analyses of threats or violent extremist messaging that provides 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 groups' intent and capabilities to attack pipeline, 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. pipelines from attacks.

[150] (TLP White) Joint Cybersecurity Advisory: *Chinese Gas Pipeline Intrusion Campaign 2011 to 2013,* (AA 21-201A, July 20, 2021.

[151] (U/SSI) FY20/21 Transportation Sector Security Risk Assessment (TSSRA) (September 2021).

[152] (U/SSI) Cyber Incidents Affecting Aviation and Surface Transportation 2021 and 2020 (Quarterly).

[153] (U/FOUO) TSA Transportation Suspicious Incident Report (TSIR) 2021 (Quarterly).

C. Security Directives

TSA issued two series of Security Directives, Pipeline-2021-01[154] and Pipeline-2021-02,[155] to enhance pipeline cybersecurity. Additionally, TSA issued an Information Circular[156] with recommendations for enhancing pipeline cybersecurity to all owner/operators of hazardous liquid and natural gas pipelines not subject to the requirements of the Security Directives. The Security Directives require critical pipeline owner/operators to: designate a cybersecurity coordinator; report cybersecurity incidents to CISA; conduct a cybersecurity vulnerability assessment; establish and implement a TSA-approved Cybersecurity Implementation Plan; develop and maintain an up-to-date Cybersecurity Incident Response Plan; and, establish a Cybersecurity Assessment Program and submit an annual plan to describe how the owner/operator will proactively assess the effectiveness of required cybersecurity measures.

The Information Circular recommends implementation of similar measures found in the SDs, such as: the designation of a primary and alternate corporate security manager; the reporting of cybersecurity incidents to CISA, the development and implementation of a Cybersecurity Incident Response Plan; and, the review and implementation of recommended actions from the Joint Cybersecurity Advisory issued on January 11, 2022, by CISA and the FBI.

II. Objectives, Activities, and Measuring Progress

The Pipeline 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 pipeline security.

[154] Security Directive Pipeline-2021-01 was originally issued on May 26, 2021, and most recently reissued as Pipeline-2021-01B on May 27, 2022.

[155] Security Directive Pipeline 2021-02 was originally issued on July 19, 2021, and most recently reissued as Pipeline-2021-02C on July 21, 2022. This Security directive continues, under a new performance-based regulatory model, mandatory cybersecurity measures first implemented by TSA in July 2021.

[156] Information Circular Pipleine-2022-01, issued February 16, 2022.

Figure 13: Pipeline Security Goals

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.1: Security Planning Reduce the risks from a terrorist attack on pipeline systems through security plans addressing critical infrastructure protection, operational practices (to detect and deter), and cybersecurity.	**Activity 1.1.1:** Review, implement, and update security and contingency plans based on risk and guidance in the TSA Pipeline Security Guidelines. (Industry/DHS/TSA) **Outcome:** Comprehensive and up-to-date security and contingency plans that reduce risk by explicitly addressing pipeline physical security policies and procedures. **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).[157] (DHS/TSA) -- **Activity 1.1.2:** For TSA-identified critical owner/operators, implement a cybersecurity contingency/response plan as required by TSA Security Directive. (Industry/DHS/TSA) **Outcome:** Comprehensive and up-to-date cybersecurity plans that reduce risk by explicitly addressing pipeline cybersecurity policies and procedures. **Performance Measurement:** Percentage of critical pipeline owner/operators whose cybersecurity contingency/response plans are compliant with the requirements in TSA Security Directives as assessed through compliance verification/inspections. (DHS/TSA)
Objective 1.2: Security Training Conduct training of employees to identify, prevent, absorb, respond to, and recover from a terrorist attack.	**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) **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. **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)

[157] TSA Pipeline Security Guidelines (March 2018, with Change 1 (April 2021) https://www.tsa.gov/sites/default/files/pipeline_security_guidelines.pdf. Accessed December 22, 2021.

NSTS Goal 1	**Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience**
Objective 1.3: Security Exercises Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency.	**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) **Outcome:** Pipeline systems and public safety agencies are better prepared to respond and recover effectively in the event of security incidents. **Performance Measurement:** Percentage of pipeline companies whose security drills and exercises meet the elements in the TSA Pipeline Security Guidelines as assessed through CSRs. (DHS/TSA)
Objective 1.4: Physical Security Measures Reduce the risks from an attack on pipeline systems through physical security measures addressing critical infrastructure protection	**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) **Outcome**: Comprehensive and up-to-date physical security measures that reduce risk by addressing site-specific security measures, assessments, barriers, and incident response. **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)
Objective 1.5: Cybersecurity Reduce the risks from a cyber-attack on pipeline systems through security measures addressing critical infrastructure protection.	**Activity 1.5.1:** For critical owner/operators identified by TSA, implement cybersecurity measures as directed by TSA Security Directives. (Industry/DHS/TSA) **Outcome:** Increase pipeline owner/operator ability to successfully detect, respond, and recover against cyber intrusions, and mitigate effects of cyber incidents on their Information and Operationally Technology (IT/OT) systems. **Performance Measurement:** Percentage of pipeline companies who are compliant with TSA-issued Security Directives, including approved Action Plans in place as assessed through compliance verification/inspections. (DHS/TSA) -- **Activity 1.5.2:** For critical owner/operators identified by TSA, conduct operational technology system cybersecurity architecture design reviews as directed by TSA Security Directives. (Industry/DHS/TSA) **Outcome:** Pipeline operator Information and Operational Technology (IT/OT) architecture is periodically reviewed to identify opportunities to strengthen security capabilities**.** **Performance Measurement:** Percentage of critical pipeline owner/operators that are compliant with TSA-issued Security Directives, including approved Action Plans in place as assessed through compliance verification/inspections. (DHS/TSA)

NSTS Goal 2	**Enhance effective domain awareness of transportation systems and threats**
Objective 2.1: Intelligence and Information Sharing Maintain and enhance mechanisms for information and intelligence sharing between the pipeline industry and government.	**Activity 2.1.1:** Provide timely, accurate, and relevant information and intelligence to enhance industry's domain awareness. (DHS/TSA) **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. **Performance Measurement:** Percentage of intelligence products delivered to Pipeline stakeholders within 24 hours of release. (DHS/TSA)
Objective 2.2: Community Outreach Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with pipeline systems.	**Activity 2.2.1:** Promote pipeline security awareness in communities surrounding critical pipeline assets and systems. (Industry/DHS/TSA) **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. **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)

III. Pipeline Operational Recovery Plan

Transportation modal security plans should include an operational recovery plan to expedite the return to operation of an adversely affected transportation system following a major terrorist attack on that system or other incident.[158]

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 is addressed in the Pipeline Security and Incident Recovery Protocol Plan required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*.[159] TSA and DOT's PHMSA, in collaboration with pipeline owner/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.

[158] 49 U.S.C § 114(s).

[159] TSA Pipeline Security Guidelines (March 2018 with Change 1 [April 2021]).

Shahn Sederberg | CDOT

Appendix D: Intermodal Transportation Security Plan

Homeland Security

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."[160] This plan recognizes postal and shipping as a sub-sector that contributes to national security and provides a risk-based, strategic approach to identify and protect those elements of intermodal transportation from disruption by terrorist attacks.[161]

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."[162] Intermodal passenger operations include a mix of ground, rail, aviation, and marine transportation. For example, 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. This plan focuses on the intermodal movement of supplies, products, mail, and parcels in supply chains.

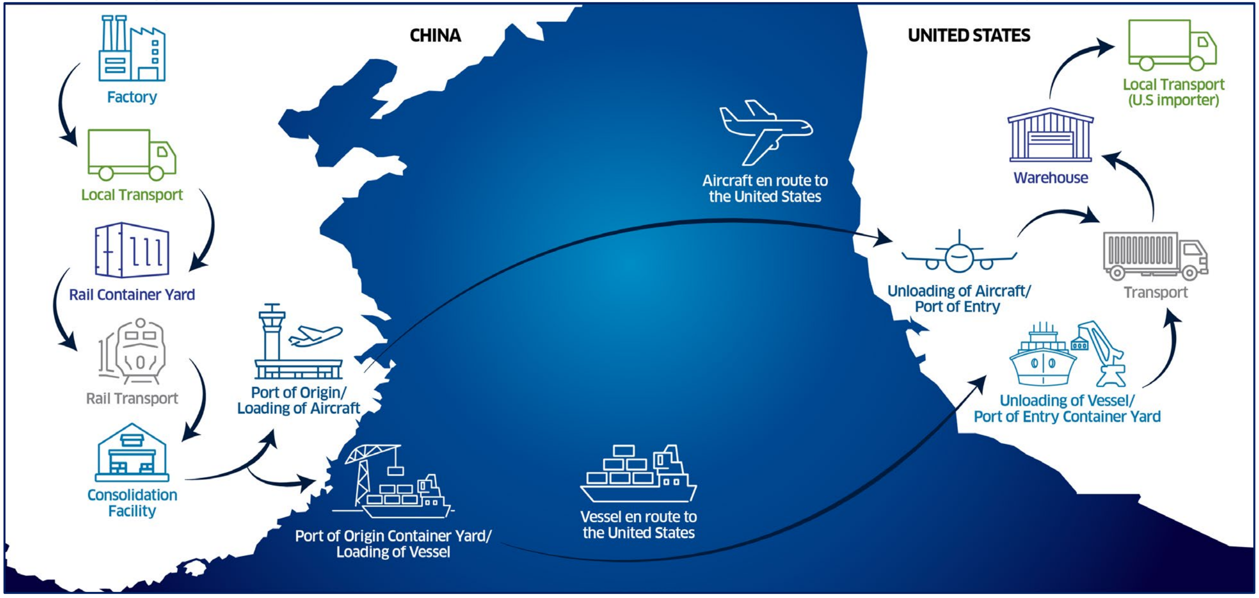
The transfer of intermodal shipments between modes usually occurs at integrated intermodal terminals as illustrated in **Figure 14**. These intermodal operations are an integral part of the global supply chain on which the U.S. depends for the efficient and secure movement of goods. The extensive web 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 that 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.

[160] 49 U.S.C. § 114(s)(3)(H).
[161] https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf. p.1. Accessed 04/14/22.
[162] Intermodal Surface Transportation Efficiency Act of 1991, Pub. L. No. 102-240, (Dec. 18, 1991).

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 safe, secure, and efficient transportation services following a disruption as quickly as possible.[163]

Figure 14: Illustrative Example of Key Points in the Global Supply Chain


CHINA
UNITED STATES
Factory
Local Transport
Rail Container Yard
Rail Transport
Consolidation Facility
Port of Origin/ Loading of Aircraft
Port of Origin Container Yard/ Loading of Vessel
Vessel en route to the United States
Aircraft en route to the United States
Unloading of Aircraft/ Port of Entry
Unloading of Vessel/ Port of Entry Container Yard
Transport
Warehouse
Local Transport (U.S importer)

1) Global Supply Chain Profile

The collective modes of trucking, rail, aviation, and maritime transportation are just some of the components that support the global supply chain system. The supply chain system is a worldwide interconnected network of millions of individual supply chains in operation at any given time. Significant transportation components 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 efficiently, rapidly, and securely.

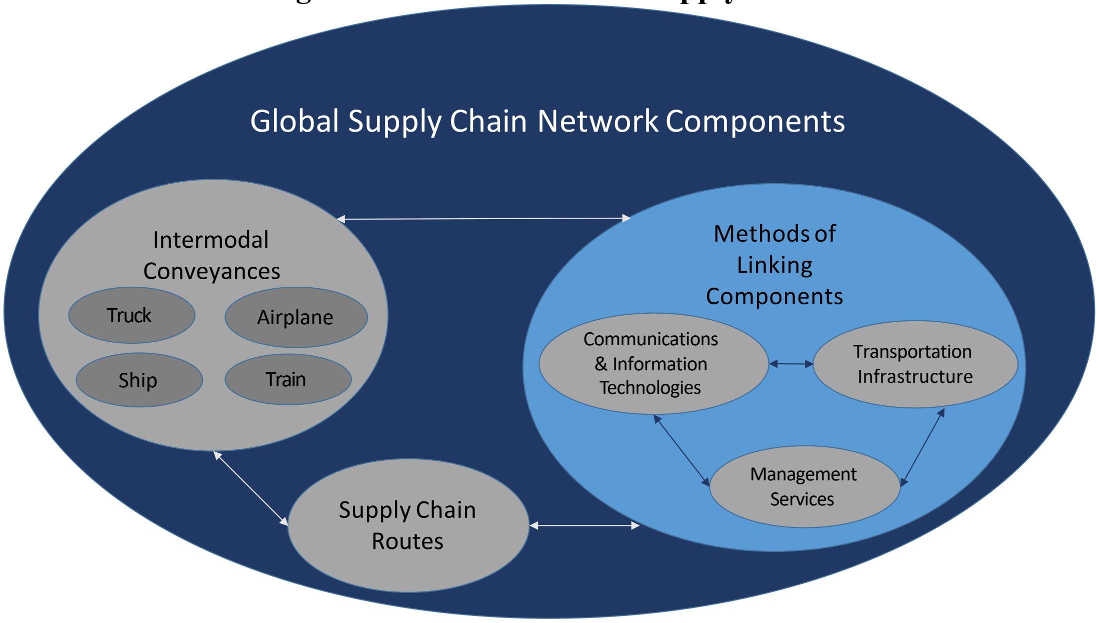
[163] 49 U.S.C. § 114(s)(3)(I).

Goods transported through supply chains are handled or managed by many entities from origin to destination, including 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 works together to monitor the independent and collective effect of transportation vulnerabilities. Individual vulnerabilities could impact the entire intermodal network.

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, secure, 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 of passengers and cargo and the 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 15**, allows for the identification of cross-cutting trends, establishment of priorities, and the identification of needs across the components.

Figure 15: Elements of the Supply Chain


Global Supply Chain Network Components
Intermodal Conveyances
Truck
Airplane
Ship
Train
Methods of Linking Components
Communications & Information Technologies
Transportation Infrastructure
Management Services
Supply Chain Routes

2) Risk Profile

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

The terrorism-related threats directed at transportation routes or assets could disrupt commodity flows, delay supplies for vital industries or medical needs, or damage or destroy critical infrastructure. Disruption of the transportation elements of critical supply chains could impact multiple sectors. The impacts could cascade 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 supply chains 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 UAS as weapons themselves (such as in the 9/11 attacks or the recent spate of truck ramming incidents in Europe and the U.S.).[164] With UAS becoming increasingly common, terrorists and other malicious actors can use them to facilitate their criminal activities, including smuggling, surveillance, and disrupting or causing damage to 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 surge 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. In addition, 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.

[164] Weapons of mass destruction: (A) any destructive device as defined in section 921 of this title 18, United States Code; (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).

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, and
- Chemicals for defense industries, public health needs, and water sanitation.

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. The following risk-based priorities for the intermodal plan mode come from analyses of congressional or executive direction, legislation, threat intelligence, risk assessments, and gap analysis.

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.

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 U.S. 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, Customs Trade Partnership Against Terrorism (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 can focus on inspection of higher-risk shipments.[165]

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, secure, and efficient flow of commerce.

[165] 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, CBP Strategic Plan, pg. 24.

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.[166] **Figure 16** 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 16: Intermodal Transportation Security Goals

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

[166] https://www.dhs.gov/national-strategy-global-supply-chain-security.

NSTS Goal 2	**Enhance effective domain awareness of transportation systems and threats**
Objective 2.1: Enhance federal analysis and sharing of transportation security supply chain information to improve situational awareness of terrorist threats.	**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) **Outcome:** Use risk segmentation methods to inform scanning decisions. **Performance Measurement:** Percent of inbound cargo identified by CBP as potentially high-risk that is assessed or scanned prior to departure or at arrival at a U.S. port of entry. (DHS/CBP)[167] **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) **Outcome**: Increase in cybersecurity domain awareness. **Performance Measurement**: Percent of assessed transportation systems sector operators implementing the NIST Cybersecurity Framework. (DHS/CISA/DOT)
Objective 2.2: Strengthen and grow stakeholder partnerships and collaboration on supply chain resilience.	**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) **Outcome:** Reduce trade delays through security process improvements. **Performance Measurement:** Percent of imports compliant with applicable U.S. trade laws. (DHS/CBP)
NSTS Goal 3	**Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce**
Objective 3.1: Manage transportation risks in the global supply chain networks to promote the efficient flow of commerce.	**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 (ACAS), and CTPAT) **Outcome:** Improve cargo flow to the U.S. through risk segmentation methods. **Performance Measurement:** Percent of cargo by value imported to the U.S. by participants in CBP trade partnership programs.

[167] (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).

NSTS Goal 3	Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce
	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) **Outcome:** Reduce trade delays through security process improvements. **Performance Measurement:** Percent of imports compliant with applicable U.S. trade laws. (DHS/CBP)

Appendix E: Mandates for the Strategy

Homeland Security

Legislative Language

The 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)
- Presidential Policy Directive 41, United State Cyber Incident Coordination (2016)
- 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 Cybersecurity Strategy (2023)

The IRTPA required the Secretary of Homeland Security to "develop, prepare, implement, and update" a National Strategy for Transportation Security.[168] 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,

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

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.

(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 U.S.C. § 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 U.S.C. § 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 systems 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

I. Acronyms

AMSC	Area Maritime Security Committee
APT	Advanced Persistent Threat
AREVE	Animal Rights/Environmental Violent Extremist
ASAC	Aviation Security Advisory Committee
ATS	Aviation Transportation System
AVE	Anarchist Violent Extremist
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 Security and 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
SD	Security Directive
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 subdivided into sub-modes. The Surface Security Plan Appendix is divided into four modal security plans to permit prioritization of risks across and within the traditional surface modal communities (49 U.S.C 114(s)(1)(B)). Each plan will address the requirements in 49 U.S.C 114(s) as explained above.

The modal security plans will be developed by the modes, using the 2020 NSTS as a baseline. The designated project leads will develop the sections of the NSTS to which they are assigned with the exception of the NSRTS and NSPTS. The Policy, Plans and Engagement (PPE) Surface Division will update the NSRTS and the NSPTS in 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 modal planners will provide updates to their modal plans via data calls. All submissions must be approved by stakeholders and cleared by leadership.

B. Analytic Approach

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

1. Analytic Teams

Analytic teams will be used to facilitate the stakeholder engagement process. The analytic teams will consist of the modal planners and appropriate stakeholders who have equities in the respective subject areas. If needed, the Strategy and Performance Branch, Strategy, Policy Coordination, & Innovation Office (SP&I) will facilitate meetings and discussions to ensure the priorities, objectives, activities and performance measures are nationally focused.

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."[169]

Government Coordinating Councils (GCCs) and Sector Coordinating Councils (SCCs) are highly regarded as key strategic partners. Modal planners are encouraged to meet private sector

[169] 49 U.S.C. § 114(s)(3)(A).

stakeholder consultation requirements through the GCC and SCC relationships already established. Advice received from the private sector through Critical Infrastructure Partnership Advisory Committee (CIPAC) related councils is not restricted by the Federal Advisory Committee Act.[170]

The NSTS, while not directly related to the "critical infrastructure security and resilience" mission, will benefit from the stakeholder communications channels and protections afforded by the CIPAC model.

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. The matrix is helpful for both planning and documenting the communications achieved during the engagement process. The matrix also provides "data" for stakeholder engagement metrics.

Vehicle/ Media	Content	Stakeholder	Frequency
Scheduled NSTS meetings	▪ Address planning challenges ▪ Provide guidance	▪ NSTS participants, others as appropriate	As necessary
Emails/iShare	▪ Informational emails ▪ Current versions ▪ Upcoming meetings	▪ NSTS participants, others as appropriate	As necessary
Transportation Sector Comments mailbox	▪ NSTS updates/ questions/concerns	▪ NSTS participants, others as appropriate	On-going

[170] 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 the Federal Advisory Committee Act.

3. Open-Source Research

The open-source research 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 CISA threat assessments; TSA Administrators Intent; FAA Modernization Act of 2018; White House national strategies, directives and executive orders; DHS strategies, plans, and directives; other assessments sources (e.g., Office of the Director of National Intelligence, Department of Defense, Department of State); and agency (e.g., 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 inform risk-based priority determinations by leadership.

4. Stakeholder Interviews

TSA and DOT conducted stakeholder interviews with government and sector coordinating council leadership, as well as designated subject matter experts regarding capabilities (People, Process, Information and Technology) needed by 2030 to address counterterrorism and enhancing system resilience. The following questions were tailored to help shape the NSTS and address the security priorities of today, tomorrow, and the future.

- How do you imagine the future transportation systems sector operating environment might change over the next 10-15 years?
- What keeps you up at night?
- What are your key assumptions about the future? How about key uncertainties?
- What are the most important skills people will need in the future?
- Given what you know today, what future capabilities does the transportation systems sector require most to remain vital (successful) in the future?
- What key transportation security indicators do you monitor on a consistent basis? Why?

5. Facilitated Joint Vision Discussion

TSA and DOT facilitated a joint vision discussion with government and industry to discuss the themes and trends that emerged from these stakeholder interviews. To follow up on the discussion, partners were asked to gauge the level of effort and level of impact, as well as barriers and challenges to address the common challenges across the Transportation Systems Sector. This information was used to update the base plan and the relevant modal plans. Project leads and modal planners used the information to provide context and verbiage to the modal plans.

The following 13 themes came from the interviews and joint vision facilitated discussion:

- Emerging Technology,
- Information Sharing,
- Cybersecurity,
- Intelligence,
- Human Capital,
- Political Climate,
- Adaption,
- Automation,
- Resources,
- Climate Change,
- Data Analytics,
- Resiliency (Supply Chain),
- Physical Security.

6. Data Calls

TSA's Strategy and Performance Branch solicited updates from modal planners through two modal specific data calls. The data calls were constructed to build upon each other. Data call 1 assisted in updating the 2020 NSTS Base Plan; data call 2 assisted in updating the modal security plans, as necessary, to align with the base plan. The data calls were 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. Risk-based priorities were considered in terms of outcomes or what the mode wanted to achieve to manage risks or reduce vulnerabilities.

a. Data Call 1: Update of 2020 NSTS Base Plan

This data call requested an update to the 2020 NSTS Base Plan, which was delivered to Congress on May 29, 2020. The 2020 NSTS was the baseline to update the NSTS. The NSTS continued the effort to "streamline" the strategy to address specific requirements in the legislation. This update includes changes, if necessary, to the strategic environment, challenges, risk-based priorities, and path forward. The information captured from the stakeholder interviews and facilitated discussion was used to provide context and language to the base plan.

b. Data Call 2: Update of Modal Security Plans

The second data call requested 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 2020 NSTS. The modal planners considered the challenges and impacts to their respective modes and recommended feasible solutions. The information captured from the stakeholder interviews and facilitated discussion was used to provide context and language to the modal plans. Also, the information regarding the level of effort and level of impact, as well as barriers and challenges to address common challenges across the transportation systems sector was used to provide further context.

Modal Profile: The modes will identify the assets that need to be protected in the interests of national security (49 U.S.C 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), as well as, other sources and factors that may be appropriate.

The team will consider the FY 2021 Risk-Based Priorities in Section 1986(a) of the *FAA Reauthorization Act of 2018* for updating priorities in the NSTS Aviation and Surface Modal Plans. However, at this time, the priorities will not be required to replace those priorities. Section 1986(a) of the *FAA Reauthorization Act* requires the TSA Administrator to annually develop risk-based priorities based on assessments conducted or received by the Secretary of Homeland Security across all transportation modes considering threats, vulnerabilities, and consequences. This report describes how TSA identified and assessed transportation security risks, developed priorities, and ranked those priorities by greatest security need. The FY 2021 Risk-Based Priorities will become part of supplementary information in Appendix F to connect the strategic alignment to the NSTS.

Objectives and Activities: Should help mitigate the risk-based priorities and accomplish the desired outcomes.

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

Performance Measures: Considering, activities reported in the 2021 Annual Report to Congress are near completion, now is the time to update any activities or measures that are not feasible or quantifiable with data. Also, identify targets or baselines for meeting the performance measures. If you are not the data owner, please make sure you are working with the data owner to develop the performance measure. As a reminder, if an activity is in the NSTS Modal Security Plan then it must have performance measure(s) that is 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/or 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. FAA Reauthorization Act of 2018, Section 1986 Risk-Based Priorities[171]

The risk-based priorities show in **Figure 17** were validated and ranked by the modal subject matter experts. To protect Sensitive Security Information, ranking and scoring information is not included in this appendix. Please refer to the FAA Reauthorization Act Section 1986 Report for the ranking and scoring.

Figure 17: Risk-Based Priorities (Across All Transportation Modes)

Across Mode Priorities	Description	Mode
Enhance Insider Threat Program	Improve efforts to detect, deter, and mitigate insider threats.	Cross-modal
Enhance Security Capabilities & Effectiveness	Invest in capabilities to establish enhanced integrated checkpoint and baggage screening capabilities, and improve in-flight risk mitigation.	Aviation
Enhance Cybersecurity Capabilities	Improve the collaboration with key partners and stakeholders toidentify, deter, mitigate, and manage cybersecurity risks to the transportation network and systems.	Cross-modal
Improve Operations Policy, Regulation, and Oversight	Develop and implement security policies, regulations, and oversight, in conjunction with strategic partners, to deploy risk-based transportation security measures to counter domestic and international threats to the aviation system.	Aviation
Enhance Air Cargo Security	Expand and strengthen air cargo security capabilities, fully execute authorities and advance partnerships and information sharing with industry and security partners.	Aviation
Advance Security Capabilities for UAS	Expand and strengthen UAS security capabilities, fully execute authorities, and advance partnerships and information sharing with industry and security partners.	Cross-modal
Improve Information Sharing	Improve security information sharing and community outreach with front-line operators, modal security partners, and the public.	Cross-modal

[171] Section 1986, Division K, Title I of the *FAA Reauthorization Act of 2018*, Pub. L. 115-254, 132 Stat. 3537 (Oct. 5, 2018)

Across Mode Priorities	Description	Mode
Expand Identity Management Practices	Enhance enrollment and vetting capabilities to address emerging threats, increase security effectiveness, and improve the quality of intelligence. Advance identity verification and validation capabilities to inform risk-based security and improve the passenger experience.	Cross-modal
Modernize Security Training	Modernize and deliver security training to prepare Aviation employees to deter, prevent, detect, and mitigate terrorist activities.	Aviation
Conduct Security Transportation Training, Planning, and Exercises	Conduct security training, planning exercises, and assessments to enhance surface transportation system resilience and recovery.	Surface
Improve Operations Policy, Regulation, Assessments, and Oversight	Enhance risk-based surface transportation security policies and guidance, and improve relationships with industry operators, TSA partners, and other federal agencies to assist in policyimplementation efforts.	Surface
Test & Evaluate Security Technology	Collect and develop data on the performance, use, and testing of technologies that increase security effectiveness of surface transportation modes.	Surface

IV. 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)

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)

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.

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)

CWMD enhances and coordinates DHS strategic and policy efforts with Federal, State, local, tribal, and territorial 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)

CISA 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 U.S. 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 (DOC)

DOC, 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 (DOT)

The mission of 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 aviation, maritime, and surface transportation.

U.S. Department of State (DOS)

DOS 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. DOS, 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

V. Glossary of Terms

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

Anarchist Violent Extremists. Individuals who seek, wholly or in part, through unlawful acts of force or violence, to further their opposition to all forms of capitalism, corporate globalization, and governing institutions, which they perceive as harmful to society. (Source: Terms and Definitions Associated with Domestic Terrorism or Domestic Violent Extremism, March 25, 2021)

Animal Rights/Environmental Violent Extremists. Groups or individuals who facilitate or engage in the unlawful use or threat of force or violence or intent to intimidate or coerce, in furtherance of political and/or social agendas by those seeking to end or mitigate perceived cruelty, harm, or exploitation of animals or perceived exploitation or destruction of natural resources and the environment. (Source: Terms and Definitions Associated with Domestic Terrorism or Domestic Violent Extremism, March 25, 2021)

Asset. Person, structure, facility, information material, or process that has value. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Consequence. Effect of an event, incident, or occurrence. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Control Systems. Computer-based systems used within many infrastructures 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 U.S., 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 U.S.A 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)

Domain Awareness, Air. Effective understanding of information, threats, and anything associated with the air domain that could impact the security, safety, or economy of the United States. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Domain Awareness, Land. Effective understanding of information, threats, and anything associated with the land domain that could affect the safety, security, commerce, or environment of the United States. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Domain Awareness, Maritime. Effective understanding of information, threats, and anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Domestic Terrorism. DHS defines domestic terrorism as any act of unlawful violence that is dangerous to human life or potentially destructive of critical infrastructure or key resources committed by a group or individual based and operating entirely within the United States or its territories without direction or inspiration from a foreign terrorist group. This act is a violation of the criminal laws of the United States or of any State or other subdivision of the United States; and appears to be intended to intimidate or coerce a civilian population, to influence the policy of a government by intimidation or coercion, or to affect the conduct of a government by mass destruction, assassination, or kidnapping. A domestic terrorist differs from a homegrown violent extremist in that the former is not inspired by, and does not take direction from, a foreign terrorist group or other foreign power. (Source: Terms and Definitions Associated with Domestic Terrorism or Domestic Violent Extremism, March 25, 2021)

Domestic Violent Extremist. An individual based and operating primarily within the United States or its territories without direction or inspiration from a foreign terrorist group or other foreign power who seeks to further political or social goals, wholly or in part, through unlawful acts of force or violence. The mere advocacy of political or social positions, political activism, use of strong rhetoric, or generalized philosophic embrace of violent tactics does not constitute extremism and may be constitutionally protected. DVEs can fit within one or multiple categories of ideological motivation and can span a broad range of groups or movements. DHS utilizes this term synonymously with "domestic terrorist." (Source: Terms and Definitions Associated with Domestic Terrorism or Domestic Violent Extremism, March 25, 2021)

Federal Departments and Agencies. Any component of the U.S. 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, 2018 Edition, Revision 04)

Hazard. Source or cause of harm or difficulty. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Homegrown Violent Extremist. A person of any citizenship who has lived and/or operated primarily in the U.S. 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, 2018 Edition, Revision 04)

Information Circular. A document that provides the transportation community with information in carrying out security duties. The ICs are based upon information concerning threats to transportation and are created per threat for each area of transportation. ICs are used to advise the transportation community at the Sensitive Security Information (SSI)-level of those threats or situations considered sufficiently serious and credible to warrant the consideration of extra vigilance and/or additional security measures. (Source: iShare: https://ishare.tsa.dhs.gov/PoliciesAndForms/recmgt/Pages/Records%20Disposition%20Schedules/1300-Intelligence.aspx)

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, 2018 Edition, Revision 04)

Lone Offender. An individual motivated by one or more violent extremist ideologies who, operating alone, supports or engages in acts of unlawful violence in furtherance of that ideology or ideologies that may involve influence from a larger terrorist organization or a foreign actor. (Source: Terms and Definitions Associated with Domestic Terrorism or Domestic Violent Extremism, March 25, 2021)

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, 2018 Edition, Revision 04)

Risk Mitigation. Application of measure or measures to reduce the likelihood of an unwanted occurrence or its consequences (Source: DHS Lexicon, 2018 Edition, Revision 04)

Security Directive: An emergency authority given to TSA in statute that enables TSA to enact mandatory measures if TSA has determined that additional security measures must be issued immediately in order to protect transportation security. (Source: 49 U.S.C. 114(*l*))

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. Group of objects or units combined to form a whole and to work together to achieve results not possible from the individual parts to achieve a given purpose.
(Source: DHS Lexicon, 2018 Edition, Revision 04)

Terrorism. Premeditated threat or act of violence, against persons, property, environmental, or economic targets, to induce fear or to 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, 2018 Edition, Revision 04)

Threat. Indication of potential harm to life, information, operations, the environment, or property. (Source: DHS Lexicon, 2018 Edition, Revision 04)

Vulnerability. A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (Source: DHS Lexicon, 2018 Edition, Revision 04)