Biennial National Strategy for Transportation Security

April 18, 2023

Homeland Security

Message from the Administrator

April 18, 2023

I am pleased to present the *Biennial National Strategy for Transportation Security (NSTS)*, a forward-looking, risk-based strategy designed to protect the Nation's transportation systems from attack or disruption by terrorists or other hostile forces over the period spanning years 2023 to 2027. The Transportation Security Administration (TSA) prepared the NSTS pursuant to title 49 of the United States Code, section 114(s), which requires a biennial update.

As the lead federal agency for transportation security, TSA manages development of the NSTS in partnership with the U.S. Department of Transportation (DOT), the U.S. Coast Guard (USCG), and in consultation with government and industry stakeholders. The NSTS is now in its ninth iteration. It is issued to guide policy and resource decisions about transportation security across the U.S. government.

The transportation community—led by the Transportation Systems Sector's co-Sector Risk Management Agencies—collaborates to carry out its collective security mission and manage risks to the transportation systems sector guided by the four following principles:

- Implementing an intelligence-driven, risked-based approach to manage threats and allocate resources while preserving the vitality of the transportation system.
- Fostering a unity of effort through a whole of community approach to ensure the free flow of commerce our Nation relies upon.
- Preserving the civil rights and civil liberties on which our Nation was founded.
- Accountability to the American people for implementing effective and efficient programs to promote the legitimate movement of people and commerce.

I look forward to working with the Congress, DOT, the USCG, as well as advisory and coordinating councils in implementing the security mission as outlined in the NSTS.

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

The Honorable Maria Cantwell
Chair, Senate Committee on Commerce, Science, and Transportation

The Honorable Ted Cruz
Ranking Member, Senate Committee on Commerce, Science, and Transportation

The Honorable Gary C. Peters
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rand Paul
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Chris Murphy
Chairman, Homeland Security Subcommittee, Senate Committee on Appropriations

The Honorable Shelley Moore Capito
Ranking Member, Homeland Security Subcommittee, Senate Committee on Appropriations

The Honorable Mark E. Green
Chairman, House Committee on Homeland Security

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

The Honorable James Comer
Chairman, House Committee on Oversight and Accountability

The Honorable Jamie Raskin
Ranking Member, House Committee on Oversight and Accountability

The Honorable David Joyce
Chair, Homeland Security Subcommittee, House Committee on Appropriations

The Honorable Henry Cuellar
Ranking Member, Homeland Security Subcommittee, House Committee on Appropriations

The Honorable Kevin McCarthy
Speaker of the House

The Honorable Steve Scalise
House Majority Leader

The Honorable Hakeem Jeffries
House Minority Leader

The Honorable Chuck E. Schumer
Senate Majority Leader

The Honorable Mitch McConnell, Jr
Senate Minority Leader

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

Sincerely,

David P. Pekoske
Administrator

Executive Summary

The Biennial National Strategy for Transportation Security addresses the security of transportation assets in the United States that must be protected from attack or disruption by terrorist or other hostile forces.[1] This strategy presents a forward-looking, risk-based plan to provide for the security and freedom of movement of people and goods while preserving privacy, civil rights, and civil liberties. It identifies objectives to enhance the security of transportation infrastructure, conveyances, workers, travelers, cargo, and operations. Moreover, the NSTS aims to provide a whole-of-government approach for transportation security from a counterterrorism and cybersecurity perspective. This strategy consists of a Base Plan and Modal Security Plans for the aviation, maritime, surface, and intermodal modes.

The NSTS seeks to secure transportation critical infrastructure including airports, railroads, pipelines, and ports, among other assets. These assets must be protected from international and domestic terrorists, Nation State, criminal and other malicious cyber actors, insider threats, and other adversaries in a continually evolving threat environment. To protect the Nation's diverse transportation assets from these varied threats, the NSTS has identified a set of risk-based priorities organized into three strategic goals. These priorities are applicable across the transportation sector, and the Modal Security Plans provide further information on how the strategic goals are implemented in each transportation mode. These priorities will guide government at all levels, industry partners, and other transportation stakeholders in taking action to improve security and address terrorism risks.

[1] 49 U.S.C. § 114(s)(3)(A).

1 GOAL 1. Manage Risks to Transportation Systems from Terrorists and Cyberattacks, and Enhance System Resilience

The transportation systems sector must be secured against a continually evolving threat environment. These threats include terrorist attacks, the weaponization of now-commonplace unmanned aircraft systems, malicious cyber activity that could lead to catastrophic operational failures, and insider threats willing to use their access to the Nation's transportation systems for malicious purposes.

Risk-based Priorities

- Enhance Insider Threat Program
- Enhance Cybersecurity Capabilities
- Enhance Weapons Detection Programs
- Responding to and Countering[2] Unmanned Aircraft System (UAS) and Autonomous Systems Threats in an Airport Environment
- Expand Identity Management Practices
- Enhance Security of Critical Transportation Assets in Public Areas
- Improve Preparedness Capabilities and Resilience

2 GOAL 2. Enhance Effective Domain Awareness of Transportation Systems and Threats

The transportation systems sector is made up of government entities, industry owners and operators, nonprofit employee labor organizations, and other stakeholders, all of whom must coordinate their activities to effectively secure the sector. This includes cooperation through intelligence sharing, security planning, and preparedness exercises.

Risk-based Priorities

- Improve Risk Assessments and Security Planning
- Improve Coordination with Intelligence and Threat Analysis Partners
- Investment in Security Training and Exercises

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

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

In addition to focusing on evolving threats, the transportation systems sector must continue to pursue strategies to provide more effective and efficient security, thereby supporting the freedom of movement of people and commerce. As the volume and tempo of transportation increases, security must continually improve to keep pace. This includes encouraging a culture of innovation, where all transportation stakeholders look for ways to improve transportation security.

Risk-based Priorities

- Accelerated Screening of Low-Risk Passengers and Cargo
- Enhancing Enterprise Cybersecurity of Transportation Systems Sector Risk Management Agencies and Industry
- Protecting Privacy, Civil Rights, and Civil Liberties During Screening

Implementing these goals and risk-based priorities will require commitment and coordination across the transportation systems sector. The Modal Security Plans provide further detail on how these goals and priorities will be achieved within each transportation mode.

The NSTS should inform other transportation security strategies, which will provide further objectives to achieve the goals of the NSTS. The strategies that should be informed by the NSTS include the DHS Strategic Plan and the DOT Strategic Plan, as well as the strategies of their component agencies. The goals and priorities of the NSTS are tied to specific outcomes, which are identified in the Base Plan and the Modal Security Plans. These outcomes provide a basis for measuring progress towards the goals of the NSTS. Finally, in addition to the goals and risk-based priorities, the NSTS includes a set of research and development topics that will help bring new solutions to security challenges in the transportation systems sector.

Biennial National Strategy for Transportation Security

Biennial National Strategy for Transportation Safety

Table of Contents

Executive Summary v

Introduction 1

The Transportation Systems Sector 2
Threat Environment 3
Risk-Based Priorities 4

Goal 1. Manage Risks to Transportation Systems from Terrorist and Cyber-Attacks and Enhance System Resilience 5

Enhance Insider Threat Program 6
Enhance Cybersecurity Capabilities 6
Enhance Weapons Detection Programs 7
Responding to and Countering UAS and Autonomous Systems Threats in an Airport Environment 8
Expand Identity Management Practices 9
Enhance Security of Sensitive (or Critical) Transportation Assets in Public Areas 9
Improve Preparedness Capabilities and Resilience 10

Goal 2. Enhance Effective Domain Awareness of Transportation Systems and Threats 11

Improve Risk Assessments and Security Planning 11
Improve Coordination with Intelligence and Threat Analysis Partners 12
Investment in Security Training and Exercises 13

Goal 3. Safeguard Privacy, Civil Rights, and Civil Liberties; and the Freedom of Movement of People and Commerce 14

Accelerated Screening of Low-Risk Passengers and Cargo 14
Enhancing Enterprise Cybersecurity of Transportation Systems Sector Risk Management Agencies and Industry 15
Protecting Privacy, Civil Rights, and Civil Liberties During Screening 15

Implementing the National Strategy for Transportation Security 16
Modal Security Plans 16
Coordination Among Stakeholders 17
Strategic Alignment 17
Performance 18
Resource and Budget Constraints 19
Transportation Operational Recovery Planning 19
Research and Development 20

Appendix A: Aviation Security Plan
Appendix B: Maritime Security Plan
Appendix C: Surface Security Plan
Appendix D: Intermodal Transportation Security Plan
Appendix E: Mandates for the Strategy
Appendix F: Supplementary Information

Introduction

The nation's transportation systems are critical to the American way of life, which makes them targets for terrorist and cyber-attacks. Transportation systems in the U.S. face threats from a broad spectrum of adversaries, including nation states and their proxies, foreign terrorist organizations, as well as more emboldened domestic violent extremists, and transnational criminal organizations. Some of the threats in this environment are well-established, for example, terrorists continue to target aviation targets with improvised explosive devices (IEDs). Other threats are newly emerging, such as concealed non-metallic weapons created by 3-D printing and weaponized unmanned aircraft systems. Cyber threats are increasing from a range of potential threat actors, posing a threat to both the information systems and operational technology (OT) increasingly used in transportation systems.[3]

In addition to the evolving risk environment, the Nation's transportation systems continue to evolve in response to changing demands, new technologies, and challenging circumstances. For example, remote and hybrid work schedules, decarbonization of propulsion, and increasing interconnection of information systems within transportation will continue to drive the evolution of the transportation sector. Innovative security technologies, collaboration between stakeholders, a well-trained and dedicated security workforce, and a proactive approach to preparedness and resilience will all play a part in this evolution.

Securing the nation's transportation systems presents a host of unique challenges. The sector includes transportation over air, land, and sea, as well as technology that ranges from cutting-edge to decades old. An effective security strategy must address the risks common to these modes and the unique risks within each mode. Transportation relies on cooperation between government and industry, from small businesses to multinational corporations, and transportation security plans must rely on and promote this cooperation. Similarly, transportation security depends on intra-government cooperation, from federal agencies tasked with securing the nation's transportation infrastructure to state, local, tribal, and territorial government entities who play a critical role in preparing for and responding to emergencies. Finally, the nation's transportation systems exist to freely move people, goods, data, and information. Also, the nation's transportation security strategy must respect the rights and liberties of its people and must not unduly burden the efficient operation of these systems. The security strategy for the nation's transportation systems must address all these challenges to be successful.

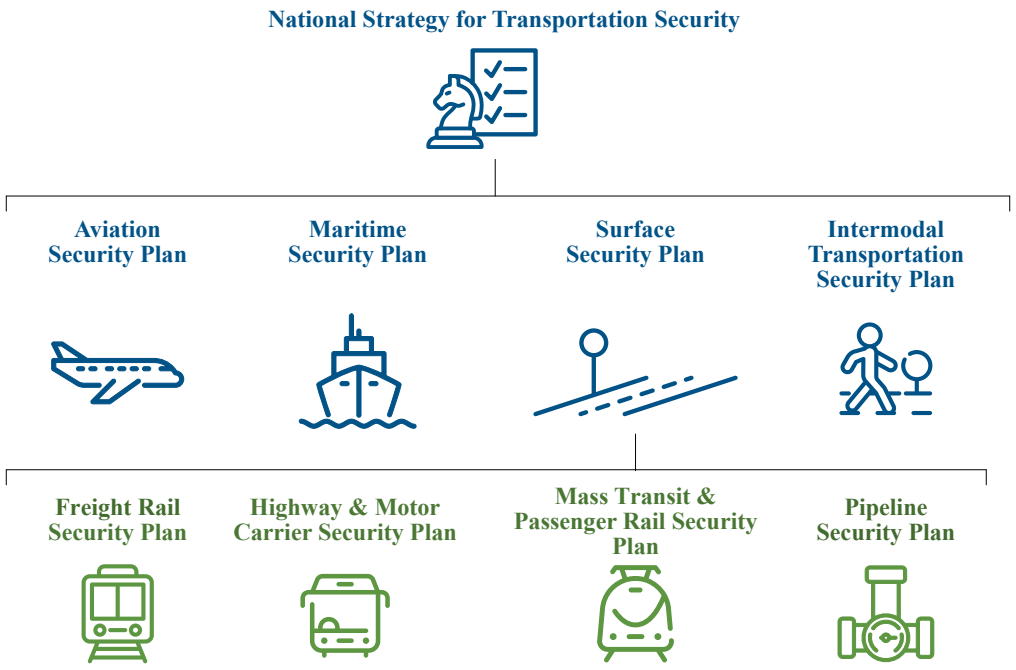
[3] This activity has included—and continues to include—nation-states carrying out cyber espionage and developing cyberattack capabilities to gain technological, political and/or economic advantages by causing localized, temporary disruptive effects on critical infrastructure, impacting the public support/perceptions, and U.S. economy.

In the face of an abundance of uncertainly, complexity and challenging times, the Department of Homeland Security and the Department of Transportation have developed the Biennial National Strategy for Transportation Security to address the security of transportation assets in the United States that must be protected from attack or disruption by terrorist or other hostile forces.[4] This strategy, for years 2023 to 2027, presents a forward-looking, risk-based plan to provide for the security and freedom of movement of people and goods while preserving privacy, civil rights, and civil liberties. It identifies priorities to enhance the security of transportation infrastructure, conveyances, workers, travelers, cargo, and operations. Moreover, the NSTS aims to provide a whole-of-government approach for transportation security from a counterterrorism and cybersecurity perspective. The NSTS also incorporates new transportation security initiatives, such as Open Architecture approach to Transportation Security Equipment systems architecture and One-Stop Security to streamline international travel.

The Transportation Systems Sector

The NSTS seeks to secure the assets of the nation's transportation systems sector.[5] The transportation systems sector can broadly be divided into seven modes: aviation, maritime, highways and motor carriers, freight rail, pipeline, mass transit and passenger rail, and intermodal. The assets within each mode include the facilities, vehicles, systems, and other infrastructure necessary for the safe and efficient movement of people and goods. These assets range from the well-established, such as jet airliners and pipeline networks, to the cutting edge, such as autonomous vehicles and Advanced Air Mobility concepts. The NSTS includes a modal plan for each of these modes, as illustrated in **Figure 1** and appended to this base plan. These modal plans more specifically identify the assets in their respective mode.

Figure 1. Modal Plans



[4] 49 U.S.C. § 114(s)(3)(A).
[5] 49 U.S.C. § 114(s)(3)(A) requires the identification and evaluation of certain at-risk transportation assets, within the NSTS.

Threat Environment

The transportation systems sector will remain a top target for malicious actors including international and domestic terrorists due to the prevalence of soft targets within the sector, the public accessibility of many transportation modes, and the importance of transportation infrastructure to the Nation. Aviation is a preferred target for terrorists seeking to conduct spectacular mass-casualty attacks that cause economic damage and garner widespread media attention. IEDs remain the preferred tactic for aircraft attacks and terrorist groups will almost certainly continue to develop innovative tactics and concealment techniques to try to get bombs onboard aircraft, however, terrorist groups also have persistent interest in a 9/11-style attack.[6] Surface transportation systems—to include mass transit, passenger rail, freight rail, pipelines, and highway and motor carriers—remain accessible targets for domestic threat actors and internationally, terrorist groups continue to promote and conduct attacks on these surface transportation targets. Increasingly, terrorist tactics involve single individuals or small teams of adversaries to orchestrate attacks on soft targets where people are densely gathered.[7] In addition to the threat of violent terror attacks, critical infrastructure is increasingly threatened with disruptive and damaging cyber-attacks, including threats to operational technology, including the positioning, navigation and timing (PNT) systems upon which transportation systems rely for safety and efficiency, that could result in catastrophic operational failures.

International threats to transportation are predominantly associated with transnational terrorist organizations, such as ISIS and al-Qa'ida. These terrorist organizations continue to pose an enduring threat from permissive operating environments.[8] In addition to foreign terrorist organizations, U.S.-based lone actors and small groups, including homegrown violent extremists (HVEs) and domestic violent extremists (DVEs) who are inspired by a broad range of ideological motivations, pose a significant and persistent terrorism-related threat to our country.[9] The transportation systems sector may be exploited by transnational criminal organizations to traffic drugs, weapons, humans, and other contraband. Illegal trafficking creates criminal networks and other adversary capabilities that terrorists can leverage through the crime-terrorism nexus to attack transportation systems. Transportation is also threatened by insiders, who may betray the trust and access granted to them in order to attack vulnerable systems as lone actors or as accomplices to other adversaries.

The transportation systems sector faces cyber risks from an array of adversaries, including state-sponsored advanced persistent threat actors (APT). Russian state-sponsored APTs have developed and deployed destructive malware throughout the ongoing conflict in Ukraine that has targeted Ukrainian critical industrial control systems and operational technology functions. The U.S. government is increasingly concerned that these APTs may engage in disruptive and destructive cyber operations and cyber-attacks against U.S. critical infrastructure in retaliation for the sanctions enacted against Russia and the provision of lethal aid to Ukraine. U.S. critical infrastructure (including transportation) is also threatened by China's robust cyberespionage capabilities and its

[6] Terrorist aviation attacks over the past decade have also targeted ground-based aviation infrastructure using a variety of tactics, including indirect fire, small arms, weaponized unmanned aircraft systems, and suicide bombings.
[7] The NSTS accounts for these types of targets and attack methods in the United States, and abroad, such as the attack at Jammu Airport in June 2021.
[8] The reemergence of permissive environments in Afghanistan following the U.S. withdrawal and the continued evolving threat across regions in Africa creates an emerging risk environment.
[9] DVEs are motivated by various factors, including racial bias, perceived government overreach and conspiracy theories promoting violence, and narratives about voting fraud in the 2020 presidential election.

ability to conduct potentially destructive or disruptive cyber operations. 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."*[10] Cyber adversaries may engage in cyber-espionage, targeting industrial secrets and other intellectual property, thereby depriving the Nation's economy of competitive advantages.

Risk-Based Priorities

Using the identification of transportation systems assets and threats to those assets as context, the National Strategy for Transportation Security is centered around a set of risk-based priorities for securing the transportation systems sector.[11] The presentation order of the risk-based priorities is not meant to denote relative priority. These priorities are organized under three goals: (1) Manage risks to transportation systems from terrorist and cyber-attacks, and enhance system resilience; (2) Enhance effective domain awareness of transportation systems and threats; and (3) Safeguard privacy, civil rights, and civil liberties; and the freedom of movement of people and commerce. These priorities should inform security decisions about the types of activities government and industry modal security officials should pursue, independently and jointly, to address terrorism risks. These priorities apply across all transportation modes, and further information about how the priorities will be carried out is presented in the modal security plans. Appendix F provides additional information on how these risk-based priorities were developed.

[10] Annual Threat Assessment of the U.S. Intelligence Community, Director of National Intelligence, 7 February 2022.
[11] 49 U.S.C. § 114(s)(3)(B) requires the NSTS to include risk-based priorities.

Goal 1. Manage Risks to Transportation Systems from Terrorist and Cyber-Attacks, and Enhance System Resilience

The transportation systems sector faces a number of evolving security risks. These risks may stem from new technology or new techniques that adversaries have adopted. For example, malicious actors may use laptops and household appliances to conceal explosives as a technique to carry out IED attacks. Evolving risks may also stem from established risks that have changed in an unexpected way. As an example, the use of unmanned aircraft systems (UAS) by adversaries is not new, but the exponential proliferation of UAS has turned it into a significant evolving risk. This was demonstrated in August 2021, when a bomb-laden UAS crashed into an airport in southwestern Saudi Arabia, wounding eight people and damaging a civil airplane—raising the possibility of such an attack occurring domestically. Other evolving risks include easier weaponization of chemical, biological, radiological, or nuclear (CBRN) agents, more sophisticated counterfeiting of identity documents, and 3-D printed weapons.[12]

Cyber vulnerabilities of operational technology is another key evolving risk. These vulnerabilities are becoming increasingly complex as owners and operators of transportation assets and systems embrace the efficiency and functionality that electronic communications and automation provide and incorporate technological components into nearly every aspect of day-to-day operations. This dependence on internet-connected devices for critical communications, financial transactions, reservations, ticketing (among other business functions), and OT, such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, for remote operability can be exploited by threat actors and introduce systemic risk. Ransomware also poses a threat to critical infrastructure and can result in downtime of operational technology, which in turn may disrupt supply chains of dependent industries and infrastructure, possibly resulting in supply shortages, economic damage, and public welfare and safety concerns. Ransomware attacks targeting U.S. networks are likely to increase in the near and long term, at least partly due to the increase of exploitable vulnerabilities in networks.

Risks also stem from cutting-edge technologies. Some innovative technologies, like advanced air mobility concepts and commercial space launch vehicles, are specific to the transportation sector, while others, like artificial intelligence and sophisticated automation, are not. These new technologies may introduce new vulnerabilities or increase existing vulnerabilities in the transportation systems sector. Other technologies, such as quantum computing and artificial intelligence,

[12] Messages or instructions in recovered terrorism manuals since 2000 show that the use of counterfeit IDs is an encouraged tactic, technique or procedure (TTP). This premise was also highlighted on page 384 of "The 9/11 Commission Report" stating, "For terrorists, travel documents are as important as weapons."

could be used by adversaries seeking to attack transportation systems sector. These risks may be relatively minor in the near term, however, the transportation systems sector should research and understand these new technologies and their associated vulnerabilities in case these risks become significant over the long term. The transportation systems sector should also leverage the work currently being done to understand and mitigate these emerging and future risks, such as the National Institute of Standards and Technology's (NIST) post-quantum cryptography efforts. Finally, these new technologies should not be viewed solely as risks, but also as potential tools for mitigating existing risks in innovative ways.

Enhance Insider Threat Program

Malicious actors employed in the transportation systems section may attack travelers, the transportation workforce, transportation assets, or transportation cyber systems. The insider threat may come from employees of transportation companies, on-site vendors, contractor personnel, or government agency employees. Recent examples include the mass shooting at a San Jose rail facility in 2021, perpetrated by an employee; and the attempted sabotage of an aircraft at Miami International Airport by a mechanic in 2019. In addition to malicious insiders, the insider threat also includes workers who unwittingly provide information to adversaries or otherwise unintentionally facilitate an attack, including cyber-attacks.[13]

To address insider threats, the NSTS emphasizes countermeasures to improve vetting capabilities, personnel security assessments, and credentialing programs. TSA is also implementing recommendations provided by the U.S. Government Accountability Office,[14] the Aviation Security Advisory Committee,[15] and the Surface Transportation Security Advisory Committee to mitigate the insider threat to transportation security.[16] For example, TSA published the TSA Insider Threat Roadmap 2020, which establishes its strategic vision to deter, detect, and mitigate insider threats in the transportation sector.

Outcome

Insider threat risks are reduced while protecting privacy in accordance with applicable laws and through the vetting of employees in security sensitive positions.

Enhance Cybersecurity Capabilities

Transportation systems rely on information systems and operational technology for business, operational, and security functions, which makes cybersecurity a key concern. Commercially-available tools enable threat actors to access these systems, including both business networks and industrial control systems, to compromise the safety of transportation operations. The ransomware attack on a major pipeline operator, which resulted in the company temporarily shutting down its pipeline system, demonstrated both the operational impact a cyberattack can

[13] "A complacent or uninformed workforce can be equally as damaging by inadvertently allowing easy access to an external threat. Malicious insiders with authorized access or insider knowledge of critical assets offers them opportunity to compromise information, sabotage infrastructure, or inflict harm upon co-workers." Cybersecurity and Infrastructure Security Agency (CISA): Fact Sheet – Insider Threat Mitigation Program, 2018.

[14] Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals | U.S. GAO.

[15] 49 U.S.C. § 44946.

[16] See Section 1969 of the FAA Reauthorization Act of 2018 ((Division K, Title I of the FAA Reauthorization Act of 2018, Pub. Law 115-254; Oct. 5, 2018), codified at 6 U.S.C. § 204.

have on a transportation system, as well as the economic impact such an attack can have on the Nation. Beyond economic impact, a cyberattack on the transportation systems responsible for the safe and efficient movement of people could result in substantial loss of life and property damage in a worse-case scenario.

The NSTS encourages critical infrastructure owners and operators in the transportation systems sector to assess the threats to their cyber systems, to collaborate in researching mitigation measures, and to invest in securing their systems. TSA has issued cyber-related Security Directives (SD) for pipelines and surface transportation, Security Program Amendments in aviation, and Information Circulars (ICs) for owners and operators in aviation, pipeline, rail, and over-the-road-bus transportation sectors not covered by the SDs and Security Program changes. TSA will continue to use lessons learned in the past year to update cybersecurity requirements and guidance; for example, TSA has already updated the pipeline SDs with improvements. TSA will further develop cybersecurity regulations for transportation critical infrastructure and has already issued an advance notice of proposed rulemaking for several surface transportation modes to inform a notice of proposed rulemaking to be published in FY 2023. Transportation cybersecurity is also promoted through the efforts of the Sector Risk Management Agencies for the transportation systems Sector.[17] The Coast Guard has issued cyber-related Circulars and Work Instructions for owners and operators in the maritime transportation sector, providing additional guidance to existing security regulations. The Coast Guard will further develop cybersecurity regulations for maritime transportation critical infrastructure and is working on a notice of proposed rulemaking to be published in FY 2023. Among other activities, the Sector Risk Management Agencies provide guidance to the sector for implementing NIST's Cybersecurity Framework, in partnership with CISA and industry stakeholders.

Outcome

The risk associated with malicious cyber activity on information systems and operational technology systems vital to the safe, secure, and efficient operation of transportation systems is reduced.

Enhance Weapons Detection Programs

Terrorist attacks on transportation assets often use an IED carried on a person, in cargo or baggage, or in a vehicle. Terrorist attacks on transportation may also make use of small arms, edged weapons, or CBRN weapons and materials. Emerging technologies, such as 3-D printing technology, provide opportunities for terrorists to attack transportation targets in ways that are difficult to detect. Terrorists acting alone or in small units can gain access to crowded terminals and other congested transportation assembly areas to perpetrate attacks using any of these weapons.

Weapons detection programs are designed to prevent the introduction of weapons of mass destruction or other lethal materials or devices into transportation systems whether carried on a person, in baggage, or in cargo. Federal agencies, state, local, tribal and territorial agencies, including law enforcement and local transit authorities, and private industry employ explosive detection canines, behavioral detection methods, and a variety of sensor, screening, and advanced information technologies to reduce the possibility that dangerous items could be introduced into aviation, maritime, and surface transportation

[17] The Sector Risk Management Agencies for the Transportation Systems Sector are the Department of Transportation and the Department of Homeland Security. In this capacity, the Department of Homeland Security is represented by TSA and USCG.

modes. As appropriate, transportation system operations will include Global Nuclear Detection Architecture (GNDA) planning, cooperation, and collaboration efforts pursuant to the SAFE Port Act.[18]

TSA will use an open architecture approach for transportation screening equipment, to improve weapons detection programs. Open architecture is an approach to system design using standardized interoperable interfaces between components, allowing many vendors to create improved components that can be easily integrated into the system, resulting in a superior transportation system. Implementing open architecture in the acquisition of transportation security equipment will allow federal transportation agencies to more rapidly respond to emerging threats and adopt industry innovations that provide unique capabilities. This will improve the likelihood of delivering enhanced capabilities to the field in a timely manner, increasing security effectiveness, operational efficiency, and passenger experience. Open architecture improves data collection, reduces costs, enhances data availability, and improves data relevance. TSA is exploring open architecture solutions for checkpoint screening equipment to improve effectiveness and message exchanges between equipment. Beyond checkpoint screening, open architecture can also be used in other transportation security contexts, such as checked baggage screening or cargo screening, to achieve similar benefits.

Outcome

The risk of weapons and other dangerous articles being carried onto public modes of transportation is reduced and the risk of WMDs being transported in commercial conveyances is reduced.

Responding to and Countering[19] UAS and Autonomous Systems Threats in an Airport Environment

UAS and autonomous conveyances are transformative innovations. However, they also pose national security challenges. Terrorists may employ them for delivery of ordnance or to otherwise facilitate terrorist activities. 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. They can be launched from anywhere and can be difficult to detect by traditional surveillance (e.g., radar). UAS also pose a threat when used recklessly or carelessly, even when the use does not have malicious intent.

The NSTS recognizes the need to assess and adapt to the UAS and autonomous conveyances systems mission area. The NSTS emphasizes the activities, processes, and systems required to respond to potential threats posed to the transportation systems sector by malicious use of UAS and autonomous conveyance systems. Federal departments and agencies will support transportation system owners and operators in preparing for and responding to UAS threats.

Outcome

TSA, federal partners, and transportation owners and operators are prepared to respond to UAS/ autonomous threats.

[18] Security and Accountability for Every Port Act of 2006, Pub. L. 109-347.
[19] TSA requires additional statutory authorities to persistently counter and mitigate UAS threats in all modes of transportation.

Expand Identity Management Practices

Terrorists and other malicious actors exploit transportation systems to prepare for and conduct attacks. Domestic and international travel facilitates the capability of terrorists, traffickers, and others planning or conducting malicious activity to carry out attacks, for example, by pre-positioning operatives or assembling a geographically-dispersed terrorist cell. Weak identity management practices can turn the Nation's transportation assets into a resource for bad actors.

Preventing known and suspected terrorists and other criminals from traveling under their true identities and preventing all passengers from traveling under false identities is therefore a top priority. This requires expanding and improving identity management practices. Robust screening, in the context of identities, and vetting of passenger identities reduces the risk of terrorists traveling under their true identities and criminals travelling under false identities.[20] This includes using automated matching of biographic and/or biometric information to watchlists and threat information, as well as using manual and automated processes to resolve potential matches and false positives.[21] Detecting passengers traveling under false identities requires secure identity management practices, including strong identity proofing during enrollment processes and strong ID authentication during identity verification. These countermeasures rely on the intelligence, security, and law enforcement communities working together, and require coordination with identity document issuers, such as state-level motor vehicle departments. Identity management practices must protect privacy, civil rights and civil liberties.

Outcome

Identity management practices prevent known and suspected terrorists from traveling, and any passenger from traveling under a false identity.

Enhance Security of Critical Transportation Assets in Public Areas

Environments that are easily accessible to large numbers of people on a predictable or semi-predicted basis with limited security are soft targets for adversaries. As an example, terrorists may conduct vehicle-ramming attacks targeting travelers at congested intermodal aviation and transit venues. Critical transportation infrastructure may also present an attractive target for terrorists if accessible. For example, terrorists may attack maritime facilities in a heavily populated port area involving especially hazardous cargo with devastating effects. Transportation infrastructure in remote areas, such as rail lines and pipelines, may be targeted by sabotage attacks.

To prevent and mitigate these types of attacks, the NSTS encourages protective actions during asset construction and operations such as structural resilience, barriers, access controls, patrols, video surveillance, and alarms. Airport designers, working with security stakeholders, should think ten to fifteen years down the road. Putting the right infrastructure in place now, saves time, energy, and financial resources in the future.[22]

---

[20] "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.

[21] National Strategy to Combat Terrorist Travel, pp 14 & 15. Homeland Security Digital Library (hsdl.org).

[22] Public Area Security National Framework, 2017.

Physical security measures should be developed to close gaps identified by risk assessments.

Outcome

Perimeters of sensitive transportation locations are not breached. Critical transportation infrastructure is secure and resilient against terrorist attacks. Security measures deter nefarious actors. Responses to attacks are effective and minimize loss of life and disruption.

Improve Preparedness Capabilities and Resilience

The security of transportation systems depends on cooperation. Security personnel, frontline employees, first responders, law enforcement officers, and other government personnel must coordinate their activities to secure transportation systems. A failure to coordinate among these groups may leave security gaps that terrorists can exploit. The NSTS recognizes that successful preparedness measures depend on well-trained and informed security personnel, frontline employees, first responders, law enforcement officers, and other stakeholders at the federal, state, local, tribal, and territorial government levels.[23] The transportation community relies on close cooperation with emergency managers to enhance preparedness capabilities for responses to a variety of threats, such as terrorists or other hostile actors, through effective partnerships and practiced and coordinated operations.

An attack—either physical or cyber—on the transportation systems sector could result in disruption of transportation services, and cascading effects on communities that depend on transportation services for work, school, day-to-day needs, and supply chain management. In addition to providing freedom of movement and facilitating commerce, resilient transportation infrastructure is also key to sustaining effective supply chains for the Nation's manufacturing, refining, and commercial sectors, as well as its defense mission. To mitigate the long-term consequences of an attack, transportation systems should prioritize resiliency, to minimize service disruption in the event of an attack. This includes the state of repair of transportation infrastructure, which is an important aspect of the system's resilience.

Outcome

Effective incident readiness contributes to resilient communities and systems.

[23] As appropriate, transportation system recovery planning and operations will conform to the resumption of trade protocols developed pursuant to section 202 of the SAFE Port Act. 6 U.S.C. § 942.

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

Securing the Nation's transportation systems requires coordination between multiple jurisdictions at federal, state, local, tribal, and territorial government levels, and between government and transportation owners and operators. Each of these entities has unique knowledge and insight into transportation security, and this information must be communicated between entities to develop effective domain awareness.[24] For example, while federal agencies may have the most current threat intelligence, owners and operators in private industry may be more informed about the vulnerabilities in their transportation assets. Information sharing between entities provides a better understanding of risk, particularly when threat and vulnerability information is combined into a risk assessment. Training initiatives apply shared information to better prevent and respond to attacks on transportation systems.

The following priorities enhance information sharing and coordination, allowing security personnel to better understand threats and manage security risks within the scope of their functions and responsibilities.[25]

Improve Risk Assessments and Security Planning

Risk-informed decision making is key to securing the transportation system. The security of the Nation's transportation systems is predicated on both a solid foundation of risk assessments and deliberate, prudent planning and evidence building to manage priority risks. Risk management and risk-informed planning must occur at corporate, municipal, state, and federal levels to secure transportation systems. These risk management practices translate the knowledge gained by collaborative intelligence and information sharing into decisions on resource allocation and security planning.

An initial step to managing security risks across all modes is to understand how transportation assets, systems, and networks may be attacked. TSA and the U.S. intelligence community assess current threats and other indicators to provide transportation owners and operators with timely and useful information to address and mitigate risks to their operations. Additional assessment of vulnerabilities and potential attack consequences enable security managers in government and industry to evaluate risks

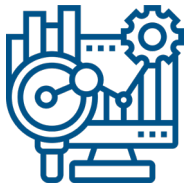
[24] Domain awareness refers to the effective understanding of information, threats, and anything associated with a domain (e.g., air, land, maritime) that could impact the security, safety, or economy of the United States. See DHS Lexicon, 2018 ed. Rev. 4 (definitions for air, land, and maritime domain awareness).
[25] 49 U.S.C § 44907.

locally, regionally, and nationally. Recurrent assessments allow program managers to evaluate the effectiveness and efficiency of risk management efforts and to adjust programs accordingly.

Allocation of resources between programs in different transportation modes should be supported by performance and program evaluations comparing those programs.[26] Although it remains difficult to draw fair comparisons between modes, as they often involve comparisons across multiple government jurisdictions and diverse industries, the government can address these challenges by creating outcome-based performance measures, focusing on outcomes common between modes, to facilitate program comparison.

Outcome

Security risk assessments are comprehensive and accurate and based on threat, consequence, and vulnerability data.



Improve Coordination with Intelligence and Threat Analysis Partners

Securing critical transportation infrastructure requires collaborative intelligence and information sharing because industry partners without intelligence warning and analysis are more vulnerable to attack. Collaborative intelligence and information sharing is necessary for industry and government security professionals to address known risks and keep pace with growing and evolving threat environments. This includes policy and strategy development, analytics, data, and information sharing capabilities for decision-making processes and procedures to ensure that information is exchanged and analyzed quickly, and that relevant, actionable information reaches all appropriate stakeholders in a timely manner.

TSA uses multiple processes, procedures, and mechanisms to disseminate intelligence and security information while complying with the Privacy Act and DHS policies. Government operation centers ensure pertinent information flows quickly to operators, government, public safety and security officials, and the public. TSA demonstrates interagency leadership in information sharing through partnership with the Sector Coordinating Councils and Government Coordination Councils. These councils and TSA resources oversee the Air Domain Intelligence and Analysis Cell (ADIAC) and the Surface Intelligence Sharing Cell (SISC), which shares intelligence with their respective stakeholders.[27] TSA is also expanding its dedicated full-time staff to work with agency partners and industry stakeholders on intelligence-sharing with the creation of the SISC. TSA will continue to support the Office of the Director of National Intelligence whole-of-government intelligence sharing efforts that encourage agencies to integrate and expand intelligence sharing tools, processes, and coordination.

Outcome

Stakeholders have accurate and timely threat information to make risk-based decisions.

[26] OMB Memorandum M-20-12, "Phase 4 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Program Evaluation Standards and Practices."

[27] This effort is under the auspices of Presidential Policy Directive (PPD)-21/Critical Infrastructure Security and Resilience and the National Infrastructure Protection Plan. ADIAC is the only full-time industry-government domain awareness effort that shares intelligence with the full support of TSA, DHS, and the Office of the Director of National Intelligence. The SISC was developed to expand information sharing with stakeholders, including unclassified and classified finished threat intelligence. Full Operational Capability is expected to be achieved in FY 23.

Investment in Security Training and Exercises

Transportation systems are threatened by motivated, experienced, and aggressive adversaries. To counter these threats, transportation systems must be secured by a professional, highly-trained security workforce and frontline personnel who are trained to counter these threats.[28] Security professionals, law enforcement officials, employees and management, and first responders must be able to work together effectively during a crisis. The layered approach to security preparedness involves multiple organizations of federal, state, and local government agencies whose rapid and coordinated actions will be essential to protect people and property. The Nation's transportation-service providers must maintain a well-trained workforce that is able to recognize, report, and respond appropriately to threats and work effectively with responders during incidents. Initial and recurrent investment in security training and exercises will be a priority for the transportation community to develop and sustain interoperability through each phase of security preparedness: prevention, protection, mitigation, response, and recovery.

Outcome

Exercise and training services build operational capacity through domain awareness and application of best practices.

[28] This includes cybersecurity professionals. See (Final March 2023) National Cybersecurity Strategy, Strategic Objective 4.6: Develop a National Strategy to Strengthen Our Cyber Workforce.

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

Federal agencies will use a data driven approach to ensure the protection of traveling passengers while promoting programs that protect privacy and safeguard personally identifiable information. The transportation systems sector must also continue to serve its purpose—allowing freedom of movement for people and goods. Securing the transportation systems sector cannot jeopardize this purpose, and security efforts must protect the civil rights and civil liberties of passengers and must not unduly burden the efficient operation of transportation services. The sector should continue to make security measures more efficient, where possible, and explore opportunities to better protect passenger rights and liberties. This effort should include investing in technologies that will benefit travelers who require modifications and need access to screening and screening support services. Further, the privacy of the transportation systems sector workforce must be protected in TSA information sharing activities associated with credentialing of the workforce.

Accelerated Screening of Low-Risk Passengers and Cargo

As transportation systems increase in speed and throughput, transportation security measures are placed under increased stress. This can place a drag on the efficiency of transportation systems if security measures cannot handle the increased pace or can create security vulnerabilities if the increased pace compromises security effectiveness.

Transportation security measures must keep pace with transportation systems to address this risk and mitigate the risk of compromised security effectiveness due to overwhelming throughput. TSA continues to pursue innovative accelerated screening of low-risk passengers and cargo to keep pace with transportation systems. Accelerated screening also improves the passenger experience and the efficiency of supply chain operations. Security officials apply technologies, data sources, and analytical methods to evaluate the risks associated with passengers and cargo and to make risk-based decisions on the necessary level of screening.

Outcome

The passenger experience is improved through innovative safety and security measures that reduce human contact with passengers and cargo and expedite screening.

Enhancing Enterprise Cybersecurity of Transportation Systems Sector Risk Management Agencies and Industry

The flow of passengers and goods in commerce requires the Federal Government and transportation stakeholders to develop and process sensitive information including, but not limited to, classified national security information, personally identifiable information, and proprietary information. This information is managed largely through government and industry information systems, which may be targeted by cyber adversaries.

Government and industry must apply strict security protocols to evaluate network infrastructure and protect sensitive information. New technologies that promote open data access, or otherwise facilitate information sharing, must be assessed for potential threats to existing protocols for maintaining the security of the transportation system.

Outcome

New technologies for systems that maintain sensitive information are assessed for threats.

Protecting Privacy, Civil Rights, and Civil Liberties During Screening

The security screening process must respect the unique personal circumstances of travelers and protect their civil rights and civil liberties. Failure to do so may infringe passenger rights and jeopardize their trust in transportation security.

The Federal Government and contract security providers use modified security screening procedures for individuals with disabilities or medical conditions. These special procedures preserve security while accommodating the unique needs of the traveler.

Outcome

Screening processes facilitate travel for passengers who require modification and reduce the impact on individual privacy.

Implementing the National Strategy for Transportation Security

Implementing the NSTS will require commitment from federal agencies tasked with securing the nation's transportation infrastructure; state, local, tribal, and territorial government entities; and private sector entities, including nonprofit employee labor organizations.[29] The Modal Security Plans, attached as Appendices A-D, provide further detail on the implementation of the NSTS within each transportation mode.

The NSTS exists within an environment of national security strategies, and its implementation requires alignment with driving strategies and execution through driven strategies. Successful implementation requires performance measurement, to ensure that the goals identified are being met. Implementation must overcome challenges, including resource and budget constraints. The NSTS also includes transportation operational recovery plans, to return transportation systems to safe, secure, and efficient operation in the event of a major terrorist attack or other incident, as well as research and development objectives to support transportation security needs.[30]

Modal Security Plans[31]

The Modal Security Plans were developed by the modal planners, using the 2020 NSTS as a baseline. The following is a synopsis of the risks outlined in the four security plans appended to the strategy. A more detailed discussion on the risks, challenges, and goals is provided for each respective mode of transportation.

The Aviation Security Plan identifies and addresses high-priority security risks to the assets and systems of the Aviation Transportation System. Multiple aviation stakeholders and government agencies protect critical aviation assets and systems, including the cyber, human, and physical elements of air cargo systems, commercial airlines and airports, general aviation, flight schools, air traffic control, and repair stations that are at the greatest risk of attack. The greatest threat to aviation security remains Improvised Explosive Devices (IEDs). Aviation risks are also generated from international and domestic terrorists, insider threats, malicious use of UAS and cyber threats.

The Maritime Security Plan presents risk-based priorities and activities to protect the marine transportation system (MTS) from terrorism and to enhance system recovery and resilience following a terrorist incident. Maritime risks stem from a mix of naturally occurring and man-made hazards and threats, including terrorist attacks, both domestic and

[29] See 49 U.S.C. § 114(s)(3)(D).
[30] See 49 U.S.C. § 114(s)(3)(F), (I).
[31] 49 U.S.C. § 114(s).

international, and cyber threats. The goals are to save lives, preserve property, and minimize disruption to the MTS and the maritime community, and protect the environment.

The Surface Security Plan includes four Modal Security Plans for mass transit and passenger rail, freight rail, highway and motor carriers, and pipelines. Attacks using small arms or edged weapons, vehicle ramming, and IEDs are likely threats to the surface modes. Public transportation is particularly susceptible to attacks using standoff weapons and CBRN agents. The surface modes rely on cyber systems for tracking, signals, and operational controls.

The Intermodal Transportation Security Plan focuses on protecting the movement of supplies, products, mail, and parcels in and across multiple modes of transportation. Transportation elements of supply chains remain vulnerable to terrorist exploitation. Disruption of the transportation elements of critical supply chains could impact multiple sectors. 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. The plan also recognizes postal and shipping as a sub-sector that contributes to national security and safeguards transportation links in the global supply chain from disruptions.

Coordination Among Stakeholders

Government and industry stakeholders—both domestic and international—work jointly to expand and improve risk-based assessments and security planning, intelligence, information sharing, supply chain, training and exercises, research and development, and technology.

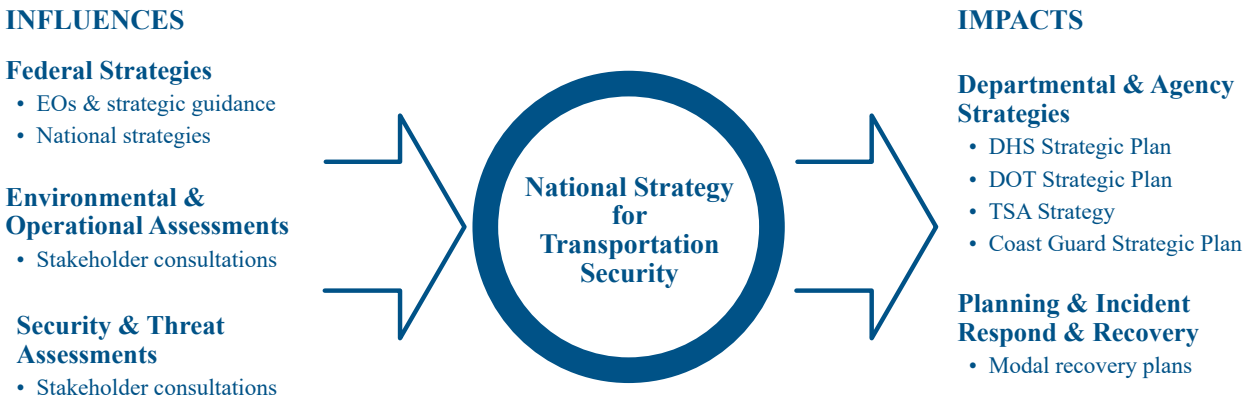
Some specific areas of focus include:

- Working with DOT, USCG, and CISA to promote partners' capabilities for protecting surface transportation systems, cyber and infrastructure, including enhancing cybersecurity capabilities and mitigations.
- Strengthening the effectiveness of TSA's aviation screening (passenger and cargo) and in-flight security operations.
- Enhancing mariner and transportation worker vetting, explosives detection, credentialing, and multi-modal security measures at ports in partnership with USCG.
- Continuing to develop appropriate capabilities to respond to threats to the transportation system from malicious use of UAS.

Strategic Alignment

The NSTS aligns with the transportation sector's current operational state. The NSTS is also based on risk assessments conducted or received by the Secretary of Homeland Security across all transportation modes. The development of the NSTS was influenced by three main sources: 1) Federal Strategies, 2) Environmental and Operational Assessments, and 3) Security and Threat Assessments. In addition, the NSTS planners conducted stakeholder interviews with government and sector coordinating council leadership and held a joint vision discussion with government and industry to discuss the themes and trends that emerged from these stakeholder interviews. The NSTS impacts departmental and agency strategies and the country's planning and incident response and recovery efforts (see **Figure 2**).

Figure 2. Influences and Impacts of the NSTS



The NSTS aligns to the National Cybersecurity Strategy in its focus on defending critical infrastructure in the transportation systems sector from cyber-threats such as APTs and ransomware criminals, as well as in its focus to improve the cybersecurity of industrial control systems and other operational technology within the sector. The cyber domain is evolving at a rapid pace, resulting in threats and mitigation measures that are changing dynamically; closing the gaps requires the expansion of traditional partnerships and collaboration efforts. Responding to cyber risk is an all of community approach; the Federal Government cannot do it alone. The cyber threat has grown exponentially in the past decade, and that growth shows no sign of slowing down. Accordingly, TSA continues to increase its capacity and capabilities to support critical mission functions to reduce the cybersecurity threat to TSS-related critical infrastructure.

Currently, TSA utilizes a multi-layered approach to enhance the sector's cybersecurity posture and improve the sector's resilience, to include: expanded cybersecurity-related assessments and reviews; cybersecurity workshops and exercises facilitated to share preventative measures, cybersecurity alerts and mitigation activities, and assessments of adopted cybersecurity-related best practices; and improved sharing of cybersecurity-related threat intelligence. In addition, due to the rapid evolution of threats and emerging technology, TSA has employed performance based, outcome-focused cybersecurity requirements for aviation, pipeline and rail (freight and passenger) owners and operators establishing expectations for baseline requirements. This approach has proven to be exceptionally agile in addressing cyber threats to the TSS and showcases best practices for other Sector Risk Management Agencies and critical infrastructure owners/operators to establish minimum requirements.

The NSTS and the National Security Strategy both recognize the threat nation states such as China and Russia pose; and that nefarious actors and foreign terrorist organizations still intend to attack the United States, while domestic violent extremism is on the rise at home. Investing in critical infrastructure, America's workforce, and innovative and emerging technologies are themes that align the NSTS with the National Security Strategy and will bolster our national and homeland security functions.

Performance

Federal, state, local, tribal, and territorial government levels, as well as industry partners, work jointly to develop a performance assessment regimen to indicate progress in achieving priority security outcomes. Progress achieving positive security outcomes is

determined by developing realistic deadlines, monitoring risk management activities, and collecting data provided by government or transportation owners and operators who are responsible for implementing the activities. Progress is reported annually to Congress on implementing the key activities in the NSTS, which is consistent with the progress reported annually in the President's Budget request.[32]

Resource and Budget Constraints

Sustaining a robust counterterrorism security and cybersecurity posture requires significant resources and funding.[33] Despite a constrained environment, the transportation systems sector is working at all levels to creatively maximize funding opportunities, including security improvements to aging infrastructure.[34] Funding plans, such as 3- and 10-year budgets, require anticipating future security programming and aligning budget projections for transportation security across multiple government departments and agencies. For example, federal funding of transportation security is largely through grants managed by DHS, Federal Emergency Management Agency (FEMA), and DOT.

Transportation Operational Recovery Planning

Mobility is essential to our way of life and a key factor in the economic vitality of the Nation. It is also a crucial component of disaster preparedness, including responding to and recovering from natural and/or human-caused disasters and terrorist and cyber-attacks. Consequently, the Federal Government, states, communities, and transportation service providers plan and prepare for response and recovery from any event that disrupts transportation. Congress required DHS and DOT to include operational recovery plans in the Modal Security Plans of the NSTS.[35] The modal operational recovery plans provide protocols for the government planners and transportation company owners and operators to consider when developing transportation recovery plans.

DOT's Recovery Resource Guide: A Transportation Stakeholder Guide to Recovery links transportation recovery processes with the principles found in the National Preparedness System, the National Response Framework, and the National Disaster Recovery Framework.[36] While these plans address the recovery of transportation systems generally, specific operational recovery protocols for the modes are provided in the Modal Security Plans which are attached to the NSTS as appendices.

Because most response and recovery actions begin, and are managed, at the local level, community involvement in the recovery planning is essential. States, regions, and communities plan and prepare for transportation response and recovery in concert with other aspects of transportation planning. DOT offers detailed guidance and protocols for transportation recovery planning on its disaster recovery website.[37] Additionally, DOT provides planning support to metropolitan planning organizations in urban locations or transportation management areas, as mandated

---

[32] 49 U.S.C. § 114(s)(4)(B).
[33] These resources are allocated towards physical security investments, research and development, planning, and recurring personnel training.
[34] This includes federal security grants to complement state, local, tribal, and territorial government and owner/operator efforts to design, develop, employ, and sustain security programs for eligible transportation systems operators and owners, and for law enforcement providers.
[35] 49 U.S.C. § 114(s)(3)(I) provides that "[t]ransportation 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."
[36] USDOT Recovery Resource Guide | US Department of Transportation.
[37] Disaster Recovery | US Department of Transportation.

by law.[38] These organizations plan for all aspects of transportation operations and infrastructure projects, including response to and recovery from emergencies.

The *Stafford Disaster Relief and Emergency Assistance Act* provides an orderly and continuing means of assistance by the Federal Government to state and local governments in carrying out their responsibilities to alleviate the suffering and damage that result from disasters. For example, it provides federal assistance programs for both public and private losses sustained in disasters. Specifically, these programs use services of all appropriate agencies to assist in developing disaster preparedness plans for mitigating, warning, emergency operations, rehabilitation, and recovery; training and exercises; post disaster critiques and evaluations; annual review of programs; coordination of federal, state, and local preparedness programs; application of science and technology; and research.[39]

Research and Development

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

The following are the research and development (R&D) priorities (not in prioritized order):[40]

- Anomaly/explosives detection
- Intrusion detection
- High-throughput threat detection
- Behavior detection and biometric identification
- Tamper protection and detection
- Blast Mitigation
- Remote disruption of attack
- System resiliency and recovery
- Interoperable information systems
- Chemical and biological threat security
- Radiological and nuclear threat security
- UAS
- Remote area detection

[38] 49 U.S.C. § 5303.
[39] Stafford Act | FEMA.gov. *Stafford Disaster Relief and Emergency Assistance Act*, February 23, 2018. (Pub. L. 100-707).
[40] 2023 Intermodal Transportation Research & Development Capability Gaps Document.


SPEED LIMIT
15