



2018 Biennial National Strategy for Transportation Security

Report to Congress

April 4, 2018



Homeland
Security

Transportation Security Administration

Message from the Administrator

April 4, 2018

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

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



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

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

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

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

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

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

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

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

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

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

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

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

The Honorable William Shuster
Chairman, Committee on Transportation and Infrastructure

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

The Honorable Mike Pence
President of the Senate

The Honorable Paul Ryan
Speaker of the House

The Honorable Mitch McConnell
Senate Majority Leader

The Honorable Chuck Schumer
Senate Minority Leader

The Honorable Nancy P.D. Pelosi
House Minority Leader

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

Sincerely yours,

David P. Pecoske
Administrator

Executive Summary

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

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

1. **Agile, Adaptable Security Posture:** Intelligence and risk assessments and forward-looking threat analyses provide the foundation to define the priorities, objectives, and activities necessary to achieve strategic goals.
2. **Partnerships:** The responsibilities for transportation services—that provide the mobility necessary for insuring prosperity and our way of life—are broadly distributed among the whole community. The Strategy recognizes that building effective partnerships, in conformance with laws for receiving advice from non-government entities, is a government responsibility.
3. **Privacy and Civil Rights:** While striving to enhance transportation security, government and industry must preserve and protect the fundamental civil rights and civil liberties of the public they serve.
4. **Accountability:** Government and private sector security partners are accountable to the American people for the implementation of this Strategy and for reporting progress.

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

¹ 49 U.S.C. § 114(s)(3)(A).

² 6 U.S.C. § 1133 and § 1161, respectively.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix A: 2018 Aviation Security Plan

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



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

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

Appendix B: 2018 Maritime Security Plan

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



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

Appendix C: 2018 Surface Security Plan

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



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

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

Appendix D: 2018 Intermodal Transportation Security Plan

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



Annexes

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

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



2018 Biennial National Strategy for Transportation Security

Table of Contents

I.	Legislative Requirement	1
II.	Introduction.....	4
A.	Purpose and Scope.....	4
B.	Guiding Principles	5
C.	Strategic Environment.....	6
D.	Challenges	8
III.	Mission, Vision, Strategic Goals, and Risk-Based Priorities.....	11
A.	Goal 1: Manage Risks to Transportation Systems from Terrorist Attack and Enhance System Resilience.....	12
B.	Goal 2: Enhance Effective Domain Awareness of Transportation Systems and Threats	13
C.	Goal 3: Safeguard Privacy, Civil Liberties, and Civil Rights; and the Freedom of Movement of People and Commerce	14
IV.	Performance	15
A.	Assessing National Transportation Security Performance	15
B.	Security Program Performance Assessments	15
C.	Strategic Performance Measures	15
V.	Path Forward.....	17
VI.	Transportation Operational Recovery Planning.....	19

I. Legislative Requirement

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

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

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

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

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

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

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

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

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

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

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

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

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

(5) Priority Status.

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

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

- (i) the current National Maritime Transportation Security Plan under section 70103 of title 46;
- (ii) the report required by section 44938 of this title;
- (iii) transportation modal security plans required under this section;

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

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

⁵ Id.

⁶ Id.

II. Introduction

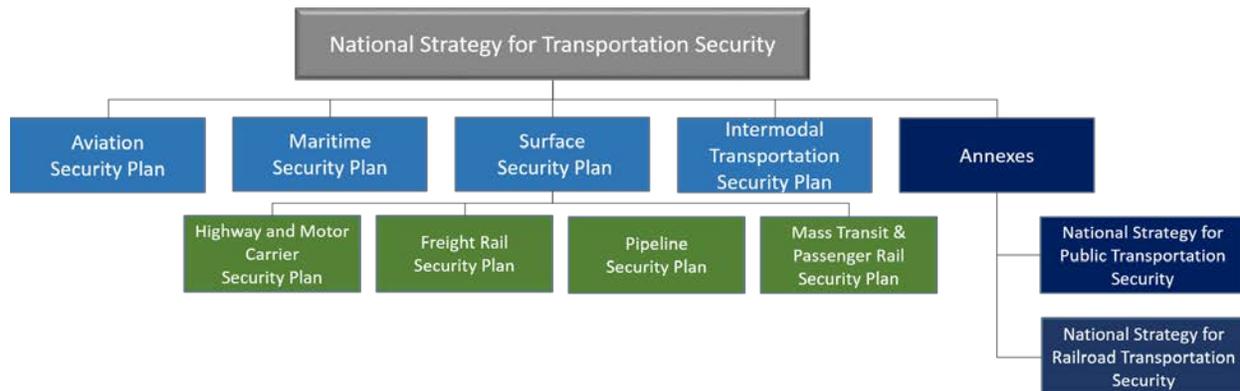
A. Purpose and Scope

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

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

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

Figure 1: NSTS Modal Plans and Strategies



⁷ Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Pub. L. No. 108-458 (December 17, 2004).

⁸ 49 U.S.C. § 114(s)(3).

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

¹⁰ 49 U.S.C. § 114(s)(5) and (6).

B. Guiding Principles

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



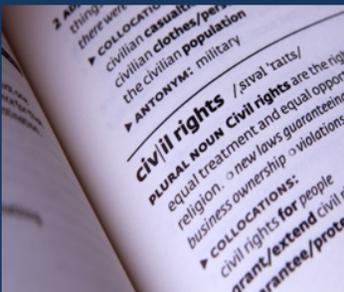
Agile, Adaptable Security Posture

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



Partnerships

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



Privacy and Civil Rights

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



Accountability

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

C. Strategic Environment

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

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

1) Assets to Be Protected

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

2) Current Risk Environment

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

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

¹¹ 49 U.S.C. § 114(s)(3)(A).

¹² <https://www.tsa.gov/news/features/2015/11/01/remembrance-gerardo-i-hernandez>.

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

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

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

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

3) Emerging Risk Environment

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

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

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

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

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

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

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

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

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

D. Challenges

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

1) Uncertainty About Risks

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

2) Resource and Budget Constraints

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

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

3) Performance Assessments

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

4) Resilience and System Recovery

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

National Preparedness Goal
Five Mission Areas*

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

* FEMA, National Preparedness Goal 2015

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

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

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

Figure 2: Development of Risk-Based Priorities

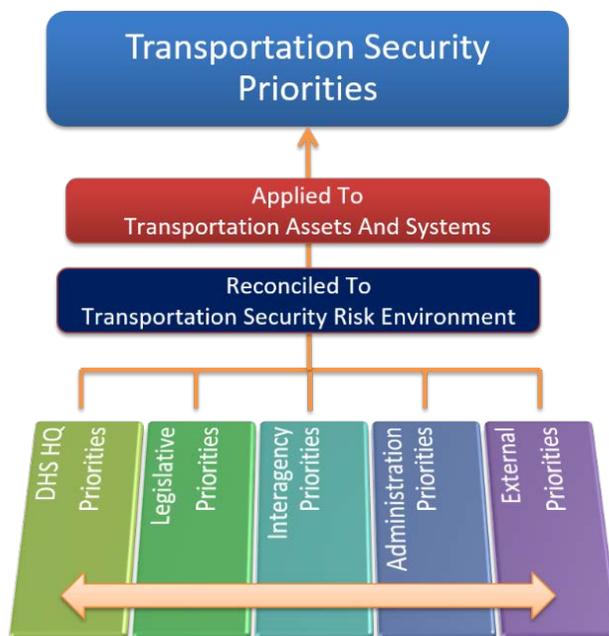


Figure 2 depicts the multiple sources used to understand the Nation’s security priorities. Congressional, executive, other governmental, and industry security priorities are considered in the context of transportation system operations. Security risks to transportation systems are aligned with national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

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

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

Risk-Based Priority 1: Physical Security

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

Risk-Based Priority 2: Weapons Detection Programs

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

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

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

Risk-Based Priority 3: Cybersecurity

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

Risk-Based Priority 4: Preventing Terrorist Travel and Insider Threats

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

Risk-Based Priority 5: Preparedness

The Strategy recognizes that successful preparedness measures depend on well-trained and informed security personnel, frontline employees, first responders, law enforcement

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

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

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

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

Source: Risk Management Fundamentals: Homeland Security Risk Management Doctrine.

Risk-Based Priority 1: Assessments

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

Risk-Based Priority 2: Information Sharing

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

¹⁴ 6 U.S.C. § 942.

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

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

Risk-Based Priority 3: Situational Awareness, Common Operating Picture

Situational awareness is required to effectively coordinate operations across the five preparedness mission areas. The Federal Government supports the enhancement of technologies and data standards that facilitate a common operating picture for decision makers to access critical and time sensitive information.

Risk-Based Priority 4: Training

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

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

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

Risk-Based Priority 1: Accelerated Screening of Low-Risk Passengers and Cargo

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

Risk-Based Priority 2: Protecting Civil Rights and Liberties during Screening

The security screening process must respect the unique personal circumstances of travelers and protect their civil rights and liberties. The Federal Government and contract security providers use modified security screening procedures for individuals with disabilities or medical conditions. These special procedures preserve security while accommodating the unique needs of the traveler.

Risk-Based Priority 3: Protecting Sensitive Information

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

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

IV. Performance

A. Assessing National Transportation Security Performance

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

B. Security Program Performance Assessments

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

C. Strategic Performance Measures

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

¹⁶ 49 U.S.C. § 114(s)(3)(b).

¹⁷ 49 U.S.C. § 114(s)(4)(c).

Table 1: Performance Measures

NSTS Goal	Risk-Based Priority	Outcome
<p>Manage risks to transportation systems from terrorist attack and enhance system resilience.</p>	<ul style="list-style-type: none"> • Physical Security • Weapon Detection Programs • Cybersecurity • Preventing Terrorist Travel and Insider Threat • Preparedness 	<p>Perimeters of sensitive transportation locations are not breached by terrorists.</p> <p>Critical infrastructure is hardened against terrorist attacks.</p> <p>Dangerous articles are not introduced into aviation.</p> <p>Weapons of Mass Destruction (WMDs) are not transported in containers.</p> <p>Chemical and biological threats are detected and neutralized.</p> <p>Terrorists are not able to travel by commercial aviation.</p> <p>Terrorists do not enter the United States.</p> <p>Transportation system employees in security sensitive positions are vetted to minimize security risks.</p>
<p>Enhance effective domain awareness of transportation systems and threats.</p>	<ul style="list-style-type: none"> • Assessments • Information Sharing • Situational Awareness, Common Operating Procedures (COP) • Training 	<p>High-risk transportation assets and systems that must be protected are routinely assessed to determine progress-mitigating vulnerabilities.</p> <p>Transportation stakeholders are satisfied with intelligence-related and other security information shared.</p> <p>Emergency responders and stakeholders have satisfactory access to incident COP.</p> <p>Exercises and training include objectives to learn about and exercise domain awareness capabilities.</p>
<p>Safeguard privacy, civil liberties, and civil rights; and the freedom of movement of people and commerce.</p>	<ul style="list-style-type: none"> • Accelerated Screening of Low-Risk Passengers and Cargo • Protecting Civil Rights and Liberties during Screening • Protecting Sensitive Information 	<p>Enrollment in TSA Pre✓[®] program and related programs is increased.</p> <p>Passenger screening time decreases.</p> <p>Policies are approved by officials responsible for protecting privacy, civil rights, and civil liberties.</p> <p>Enrollment in Customs-Trade Partnership Against Terrorism (C-TPAT) and related programs is increased.</p> <p>Cargo delays are minimized.</p> <p>Enhance the travel experience of persons with special needs.</p>

V. Path Forward

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

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

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

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

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

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

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

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

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

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

VI. Transportation Operational Recovery Planning

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

DOT's Recovery Resource Guide: A Transportation Stakeholder Guide to Recovery¹⁸ links transportation recovery processes with the principles found in the National Preparedness System (NPS), the National Response Framework (NRF), and the National Disaster Recovery Framework (NDRF). While these plans address the recovery of transportation systems generally, specific operational recovery protocols for the modes are provided in the modal security plans, attached to the Strategy as appendices.

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

¹⁸ https://www.transportation.gov/sites/dot.gov/files/docs/RECOVERY%20RESOURCE%20GUIDE_Final%20Version_08-27-2014.pdf. Accessed May 4, 2017.

¹⁹ <https://www.transportation.gov/disaster-recovery>. Accessed May 4, 2017.

