2014 National Strategy for Transportation Security

Report to Congress

April 17, 2015

Homeland Security

Transportation Security Administration

Message from the Acting Administrator

April 17, 2015

I am pleased to present the 2014 National Strategy for Transportation Security. The Strategy was prepared pursuant to a requirement in the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) as amended. It presents a forward-looking, risk-based plan to protect the Nation's transportation systems from terrorist attack over the period spanning 2015-2018. The Act requires a biennial update.

The Transportation Security Administration 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 federal, state, local, tribal, and territorial government partners and with 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.

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 Thomas R. Carper
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable Richard C. Shelby
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 Joseph R. Biden, Jr.
President of the Senate

The Honorable John A. Boehner
Speaker of the House

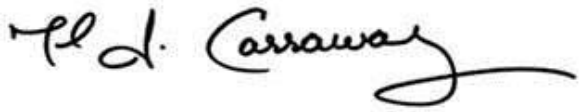
The Honorable Mitch McConnell
Senate Majority Leader

The Honorable Harry M. Reid
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.

Sincerely yours,



Melvin J. Carraway
Acting Administrator
Transportation Security Administration

Executive Summary

The 2014 National Strategy for Transportation Security (NSTS) addresses the security of "transportation assets in the United States…that must be protected from attacks by terrorists or other hostile forces."[1] The NSTS presents a forward-looking, risk-based plan to protect the freedom of movement of people and goods while preserving civil rights, civil liberties, and privacy; it identifies priority objectives to enhance the security of infrastructure, conveyances, workers, travelers, and operations. It includes a base plan that establishes the risk-based foundation for developing the strategy and the modal security plans, including the transportation sector's risk profile, guiding principles, strategic goals and objectives, cross modal priorities, and the challenges. The appended modal security plans for Aviation, Maritime, Highway and Motor Carrier, Mass Transit and Passenger Rail, Freight Rail, and Pipelines, together with an intermodal security plan, provide strategies to reduce terrorism risks and to protect travelers, workers, and goods.

Risk Profile: The NSTS 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. Threats are directed at domestic and international transportation operations. International threats are predominantly associated with transnational and regional terror organizations such as al-Qa'ida. While domestic threats to transportation have been limited in the past decade, the NSTS assumes that the attack methods and targets used overseas provide insights regarding the intent and capabilities of adversaries.

Guiding Principles: The resources to manage risks are constrained. Applying a risk-based security approach will provide a proper balance of resources to combat security challenges. Also, securing the transportation system requires effective partnerships involving the contributions and support of all levels of government, industry, and stakeholders. Activities to manage security risks must not unduly impinge on civil liberties or privacy rights and must avoid violations of civil rights.

Goals: The NSTS 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 attack 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.

Cross Modal Priorities: Protecting transportation infrastructure from terrorism involves several core security priorities that apply to all modes:

[1] 49 U.S.C. § 114(s)(3)(A)

Risk-Based Security: Risk management principles, including risk segmentation methods, are sound business practices not only for identifying threats and priorities, but also for evaluating courses of action that provide the best solutions for the cost.

Information Sharing: The Transportation Security Information Sharing Environment, an annual information sharing plan required by the 9/11 Act, provides effective policies and procedures for sharing information among government, public and private stakeholders.

Research and Development: TSA engages federal partners and industry in the Transportation Research and Development Working Group to determine priorities to close capability gaps. The priorities are submitted to DHS' Science and Technology Directorate for consideration in the Department's R&D planning process.

Cybersecurity: The Transportation Cybersecurity Strategy calls for enhancing awareness of cyber threats. To prevent systems vulnerabilities to attack or degradation, TSA strives to maintain high cybersecurity standards and encourages transportation providers to incorporate cybersecurity best practices including the National Institute of Standards and Technology Cybersecurity Framework.

Explosives: Improvised Explosive Devices (IEDs) remain one of the most accessible weapons for terrorists to damage critical infrastructure and inflict casualties.

Chemical, Biological, Radiological, and Nuclear Threats: Chemical, Biological, Radiological, and Nuclear threats to transportation systems are associated with high consequences because these systems can involve large concentrations of people, often in enclosed spaces. Moreover, cargoes such as bulk foods may be contaminated by chemical or biological agents. Bulk toxic or volatile chemical cargoes may be exploited for use as weapons.

Performance: TSA submits an annual progress report to Congress on the implementation of the NSTS. Representative activities are measured to show progress towards achieving NSTS goals.

Challenges and Path Forward: This Strategy identifies four challenge areas that transportation security partners must consider: the evolving threat, system resilience, effective risk-based assessments, and cybersecurity. Each area requires collaboration to achieve a common understanding of challenges, impacts, and feasible solutions.

Aviation

The Aviation Security Plan provides a strategic approach to address high priority security risks to the Aviation Transportation System. Aviation organizations and agencies share responsibility for protecting critical aviation infrastructure and systems and for the resilience of the Aviation Transportation System. The aviation risk profile is dominated by international and transnational terrorism. The aviation mode relies on threat intelligence and risk assessments to determine priorities, including protecting aviation physical infrastructure, assets, and cyber systems; optimizing air domain awareness of domestic and international threats among security partners;

and improving international partnerships and security cooperation to increase aviation security worldwide.

Significant improvements in aviation security are being realized through risk-based security while improving freedom of movement for travelers and commerce. However, challenges include the persistence and adaptability of terrorists and the development of new technologies such as Unmanned Aircraft Systems and non-metallic weapons.

Maritime

The Maritime Security Plan presents risk-based priorities and activities to protect the Marine Transportation System from terrorism and to enhance system recovery following a terrorist incident. Terrorism threats to the assets and systems of Marine Transportation Systems include IEDs, Weapons of Mass Destruction, standoff weapons, and cyber attacks. Cruise ships and ferries face similar IED threats as well as threats of attacks using small arms, or the release of biological or chemical agents.

The United States Coast Guard's Maritime Security Risk Analysis Model assists maritime security managers in evaluating strategic, operational, and tactical risks and establishing security priorities including increased enforcement of Maritime Security Regimes, enhanced Maritime Domain Awareness, and risk-based deployment of Maritime Security and Response Operations.

Surface

The Surface Security Plan includes modal plans for Freight Rail, Mass Transit and Passenger Rail, Highway and Motor Carrier, and Pipelines. IED attacks are the most likely threat to the surface modes. Public transportation and recreational travel are also susceptible to attacks using standoff weapons, small arms, or biological or chemical agents. Cyber threats also increase risk due to the reliance on cyber systems for tracking, signals, and operational controls

The surface modes share common security priorities to address common risks. TSA is leading collaborative efforts to establish requirements for security plans, assessments, and training programs in high-risk transportation operations. Federal partners will continue efforts to provide timely, usable threat intelligence and security information, to encourage voluntary adoption of best practices to improve cybersecurity, establish methods to measure progress achieving security objectives, and inform decisions on risk-reduction activities.

Intermodal

The Intermodal Security Plan focuses on protecting the movement of supplies and products by the multiple modes of transportation. It covers the transportation elements of the global supply chain and the delivery of goods from origin to destination by multi-modal postal and parcel shipping services. The global supply chain consists of a dense network of routes and carriers operating efficiently to provide on-time deliveries.

Threats to intermodal transportation links of the supply chain are the same as those for the modes serving the supply chain. The threats include the potential delivery of explosives, dangerous chemicals, or biological agents to specific targets. While the direct consequences of attacks on intermodal transportation may be limited, the indirect costs of attack-related system disruptions could have significant and lasting effects.

2014 National Strategy for Transportation Security

Table of Contents

I. Legislative Language

This report responds to the transportation strategic planning requirement set forth in Section 1202(b) of the Intelligence Reform and Terrorism Prevention Act, codified in title 49 of the U.S. Code. Specifically, 49 U.S.C. § 114(s), states:

> (1) The Secretary of Homeland Security shall develop, prepare, implement, and update, as needed,
> (A) a National Strategy for Transportation Security; and,
> (B) transportation modal security plans addressing security risks, including threats, vulnerabilities, and consequences, for aviation, railroad, ferry, highway, maritime, pipeline, public transportation, over-the-road bus, and other transportation infrastructure assets.
>
> (2) Role of Secretary of Transportation. - The Secretary of Homeland Security shall work jointly with the Secretary of Transportation in developing, revising, and updating the documents required by paragraph (1).

This report also responds to the content requirements set forth in the 9/11 Act. Section 114(s)(3) of title 49, United States Code, states:

> (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.
> (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.

Concerning subsequent versions of the Strategy, the legislation states, "the Secretary of Homeland Security shall submit the National Strategy for Transportation Security, including the transportation modal security plans and any revisions…to appropriate congressional committees not less frequently than April 1 of each even-numbered year."

In carrying out the responsibilities in the legislation, the Secretary "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."

The Strategy is based on law as well as executive and DHS policy, including but not limited to the following:

- Aviation and Transportation Security Act (Pub. L. No. 107-71)
- Intelligence Reform and Terrorism Prevention Act (Pub. L. No. 108-458)
- Implementing the Recommendations of the 9/11 Commission Act (Pub. L. No. 110-53)
- National Strategy for Maritime Security and its supporting plans
- National Strategy for Counterterrorism
- National Strategy for Global Supply Chain Security
- 2014 Quadrennial Homeland Security Review

Source materials include a number of directives and planning documents specific to the six transportation modes and to the postal and shipping sub-sector.

II. Sector Risk Profile

Since 9/11, there have been no successful terrorist attacks against the national transportation system, but the number of plots and disrupted attacks shows the threat remains dynamic and adaptive. The National Strategy for Transportation Security (NSTS) takes into consideration the evolving nature of the terrorist threat and the challenges posed by a more dispersed and less visible enemy. The transportation counterterrorism mission is intelligence-driven and relies on the rapid exchange of threat information across government and with industry.

Transportation assets may be the target of terrorists, or may be used by terrorists as weapons. The Transportation Security Administration's (TSA's) Transportation Sector Security Risk Assessment addresses a wide variety of aviation and surface transportation risks using terrorist attack scenarios to evaluate modes and classes of assets.[2] The United States Coast Guard (USCG) uses its Maritime Security Risk Analysis Model to evaluate maritime security risks. In addition to the TSA and USCG assessments, the NSTS priorities reflect other additional threat and risk assessments by DHS, the Department of Defense (DOD), the Federal Bureau of Investigation (FBI), and the Intelligence Community.

Both international and domestic terrorists threaten the transportation system. International threats to transportation are predominantly associated with transnational terror organizations, such as al-Qa'ida. Overseas attacks indicate aviation, public transportation, and pipeline assets are likely targets. The NSTS assumes attack methods and targets selected overseas provide insights regarding adversary intent and capabilities which may be domestically employed. Of particular concern is the potential for individuals or small groups inside the United States who are radicalized to violence to use these methods to attack transportation assets.

Explosives concealed on persons or in packages, baggage, cargo, or conveyances present the greatest risks to transportation systems. The sector is also vulnerable to attacks using stand-off weapons such as small arms, rifle- or rocket-propelled grenades, or man portable air defense systems. Additionally, certain food products such as bulk liquids and fresh consumables, when in transit, are vulnerable to intentional contamination by chemical, biological, or radiological agents. Terrorists continue to seek out and develop innovative ways to thwart security measures. Shared intelligence, vigilance, and rapid adjustment of security protocols are essential to address these evolving threats.

The openness of the transportation system and the free movement of people and goods create unique security challenges and vulnerabilities. Terrorists acting alone or in small units may gain access to sensitive or crowded areas to perpetrate attacks using explosives and small arms, as in the attacks in Mumbai, India and in the Westgate Mall in Nairobi, Kenya. Homegrown violent extremists also pose a risk to the Nation's transportation system, in that they can plan and conduct attacks with less risk of detection.

[2] Transportation Sector Security Risk Assessment (TSSRA) 3.0 2014

Even while attacks using conventional explosives remain more likely, terrorists have shown interest in obtaining and using weapons of mass destruction. Due to the accessibility of the underlying technologies associated with biological and chemical weapons and the catastrophic consequences of radiological and nuclear attacks in heavily populated areas, these weapons remain a significant risk.[3]

Cyber threats are evolving and growing more frequent; however, terrorism-related cyber attacks have not been directed at U.S. transportation systems thus far. Nevertheless, cyber threats to transportation are a growing security concern due to:

- The dependence of transportation on cyber systems for operations, access control, communications, positioning, navigation, and tracking;
- The rapid expansion of applications remotely accessing sensitive systems; and
- The increasing sophistication of adversaries.

[3] DHS 2014 Quadrennial Homeland Security Review (QHSR), p. 47 *et seq*., and p. 62 *et seq*.

III. Guiding Principles

Managing risk in constrained environment: Security does not come without 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 will apply risk segmentation methods to adapt security processes for low risks while sustaining appropriate procedures for higher risks.

Building effective 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. 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 preserve the freedom of movement and vitality of commerce on which our nation relies.

Respecting privacy, civil rights, and civil liberties: The activities undertaken by security authorities should 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 Sector's 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 NSTS provides outcome-based measures to indicate the sector's progress reducing risks; increasing awareness; and protecting privacy, civil rights and civil liberties.

IV. Sector Mission, Vision, Goals, and Objectives

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

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

Strategic Goals and Objectives:

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

- **Objective 1**: Improve transportation preparedness to mitigate, detect, respond, and recover from terrorist attacks.
- **Objective 2**: Apply risk segmentation methods to reduce risks associated with dangerous people or articles.
- **Objective 3**: Improve physical and cyber security of nationally-significant transportation infrastructure.
- **Objective 4**: Increase industry involvement in the Research and Development (R&D) process.

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

- **Objective 1**: Improve the quality and timeliness of intelligence and information products for industry and public awareness.
- **Objective 2**: Improve situational awareness of multi-domain risks associated with cross sector, regional, and intermodal dependencies.
- **Objective 3**: Expand domain awareness through risk segmentation analyses across the travel and trade system.

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

- **Objective 1**: Protect privacy, civil liberties, and civil rights of the traveling public and those involved in supply chains to the maximum extent possible, consistent with effective security policies and activities.
- **Objective 2**: Apply risk-based security approach to supply chain and traveler movements to safeguard and expedite lawful trade and travel.

V. Cross Modal Priorities

A. Risk-Based Security

> "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.*

The transportation community assesses terrorism risks based on evaluations of threat, vulnerability, and consequence related to attack scenarios. These assessments assist security managers in industry and government in determining priorities and the ways to manage priority risks. DHS uses the Risk Assessment Process for Informed Decisions to provide information to decision makers on homeland security risks and on the effectiveness of proposed risk-reduction programs. The USCG uses the Maritime Security Risk Analysis Model (MSRAM) to provide strategic and tactical risk information. The Freight Rail Mode uses the Rail Corridor Risk Management Tool. TSA's Risk-Based Security initiatives advance the concept of risk segmentation. DHS's 2014 Quadrennial Homeland Security Review identified "a risk segmentation approach to securing and managing flows of people and goods into and out of the United States" as a strategic priority.[4] "Segmenting flows of people and goods…permits more focused strategies and more efficient allocation of resources."[5] For example, several Risk-Based Security initiatives at airport checkpoints use information gained during pre-screening and through other assessments to determine the proper level of screening for a passenger's level of risk.

TSA Pre✓®, Managed Inclusion, and age-related protocols allow individuals with a lower risk profile to receive expedited screening and permit resources to be directed to unknown or higher risk passengers. U.S. Customs and Border Protection (CBP) applies risk-segmentation principles to traveler vetting and applies a similar logic in the Automated Targeting System to identify high-risk containers. The cross modal priorities are:

- Increase the use of risk-based security and risk segmentation analyses to improve security decisions; and,
- Expand awareness of risk-based security principles within the sector to facilitate common understanding of this approach to address priority risks.

B. Information Sharing

Information sharing applies to the receipt, analysis, and distribution of transportation security information "related to risks to the transportation modes…and may include specific and general

[4] 2014 QHSR, p. 53.
[5] Ibid. p. 55.

intelligence products, as appropriate."[6] As described in the National Preparedness Goal, intelligence and information sharing is a core prevention and protection capability comprised of three elements: anticipating threats; sharing relevant, timely, and actionable information; and ensuring access channels for incoming information.[7] These elements apply across a variety of types of security information including vetting encounters, threat intelligence, risk-related assessments and analyses, security policies, best practices, and operating status and conditions. Effective information sharing provides decision makers with the situational and domain awareness that enable government and industry to manage security risks effectively.

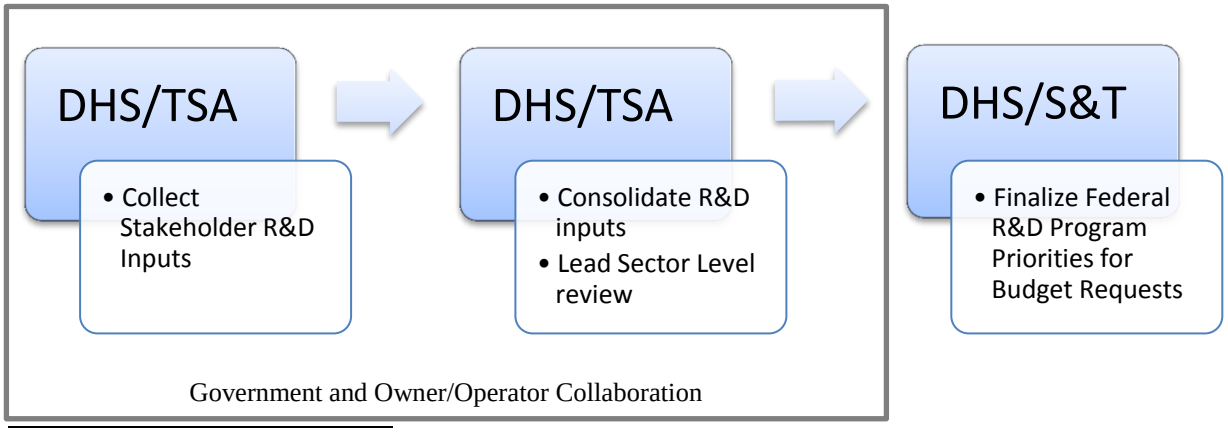
TSA prepares and annually updates the Transportation Security Information Sharing Environment required by the 9/11 Act.[8] This information-sharing environment facilitates multi-directional sharing of transportation security information and promotes trusted partnerships across the sector to ensure the right people have the necessary information when needed.

Key participants in the information sharing process are the information sources, the collectors, the analysts, the disseminators, and the users. TSA is the primary federal agency responsible for receiving, assessing, and distributing transportation-related intelligence and security information. However, information flows through multiple channels including Information Sharing and Analysis Centers, Joint Terrorism Task Forces, and fusion centers.

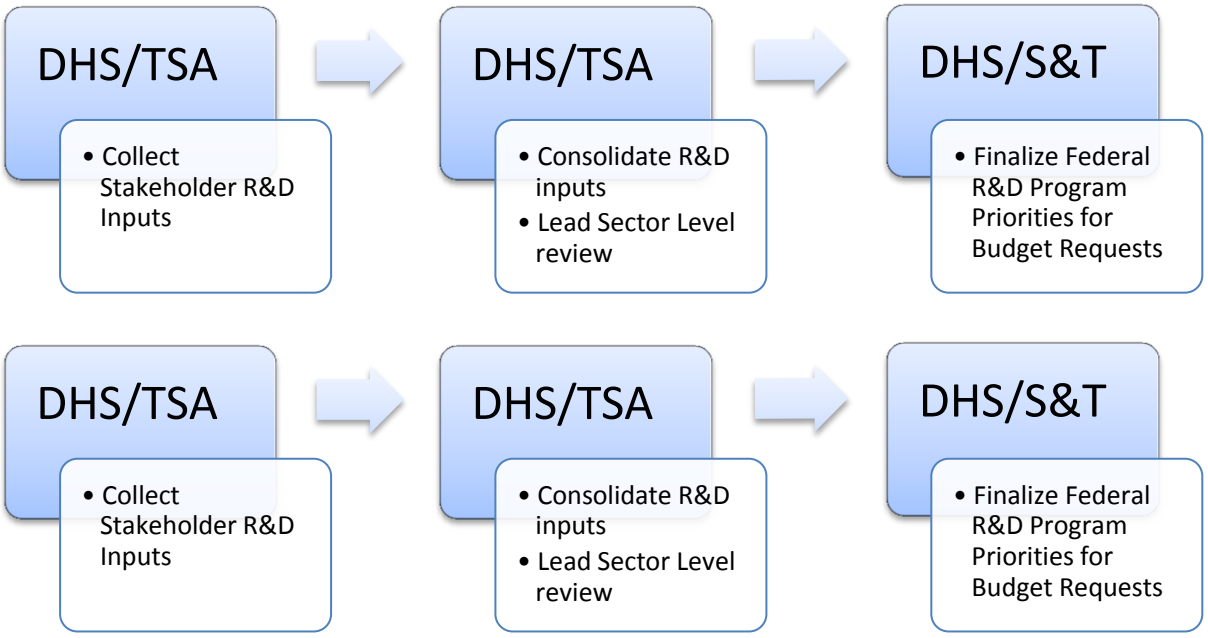
C. Research and Development

Government and industry security partners annually identify transportation security needs that cannot be met due to a lack of capabilities. Several partnership mechanisms allow capability gaps to be identified for consideration by the joint Transportation R&D Working Group. The R&D Working Group proposes prioritized R&D projects for consideration by the Department of Transportation (DOT) and DHS Science and Technology Directorate. Industry participation in identifying capability gaps and recommending priorities is encouraged, while reserving the final decisions on R&D programming to the responsible funding authorities.

Figure 1: Research and Development Framework



[6] 9/11 Act Sec 1203 (49 USC 114(u)).
[7] 2011 National Preparedness Goal, pp. 6 and 8.
[8] Implementing the Recommendations of the 9/11 Commission Act of 2007



Priority objectives for transportation R&D are based on threat and vulnerability assessments and gaps in protection capabilities. Capability gaps represent the difference between current capabilities and those needed to perform mission critical objectives. Technology capability gaps focus on:

- Surveillance, Intrusion, and Anomaly Detection Technologies;
- High Throughput Threat Detection Capabilities;
- Chemical, Biological, and Radiological Threat Detection;
- System Resilience and Recovery Capabilities;
- Remote Disruption of Attack Capabilities; and,
- Risk Segmentation Identification and Tracking Capabilities.

D. Cybersecurity

This section addresses risk management of the cyber risks posed by terrorists. Cyber vulnerabilities within transportation industries vary greatly in scope and consequence. Although the threat of a terrorist-related cyber attack causing significant loss to the function of transportation systems is low, there is potential for exploitation of cyber vulnerabilities in unanticipated ways with unforeseen consequences. For example, adversaries could use commercially available tools to hack into control systems to compromise the security and safety of transportation operations.

> 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 Programs Directorate, Office of Cyber and Infrastructure Analysis.*

The Sector's partners developed a Cybersecurity Strategy in 2012.[9] This Strategy supports Executive Order (EO) 13636 *Improving Critical Infrastructure Cybersecurity* and calls for enhancing cybersecurity awareness and promoting voluntary, collaborative, and sustainable community action. The centerpiece of the voluntary, risk-reduction strategy is awareness. Recognition of the type and extent of potential threats to infrastructure and system operations is essential for owners and operators to understand the risks and to commit the resources to offset them. The Transportation Systems Sector is also working to apply the National Institute of Standards and Technology-led Cybersecurity Framework to the various elements of the National Transportation System.

E. Explosives

IEDs remain one of the most accessible weapons available to terrorists and criminals to damage critical infrastructure and inflict casualties, as demonstrated in the wars in Iraq and Afghanistan and a series of attempted bombings of aviation dating back to 2009.. The tactics used in IED attacks continue to evolve as our adversaries seek to overcome countermeasures. The Federal Government is building upon existing policy and strategy to establish and implement measures to detect and prevent IED attacks and their consequences. The threat from IED use will remain a concern in the coming decade and will evolve in response to countermeasures. A whole-of-community approach will best position the United States to discover plots to use IEDs before those threats become imminent. High-risk transportation industries have security plans, training programs, awareness campaigns, and response protocols to prepare workers and travelers to recognize and report suspicious packages and items. DHS's "If You See Something, Say Something™" campaign broadly informs and invites the public to be aware of their surroundings and to report unusual or suspicious items.[10] Transportation industries, in partnerships with DHS, TSA, and USCG, participate in several similar initiatives such as First Observer, Airport Watch, and America's Waterway Watch.[11] These initiatives encourage transportation industry employees, travelers, and private users across the country to participate in safeguarding the transportation system. Priorities to reduce the risk from attackers using explosives are to sustain screening and detection programs using risk-based principles, to increase participation in suspicious incident reporting, and to expand detection capabilities through technologies and standard practices.

F. Chemical and Biological Threats

Public transportation and recreational travel industries frequently handle large numbers of people in confined spaces. These venues expose travelers and workers to the threat of a release of a chemical or biological agent. The consequences of such an attack are potentially devastating

[9] Transportation Systems Sector Cybersecurity Strategy, February 15, 2012

[10] The campaign was originally used by New York's Metropolitan Transportation Authority, which has licensed the use of the slogan to DHS for anti-terrorism and anti-terrorism crime-related efforts.

[11] The Aircraft Owners and Pilots Association partnered with TSA to develop the nationwide Airport Watch Program, which encourages volunteers from more than 600,000 pilots to receive security training and to watch for and report suspicious activity.

even though the likelihood of their occurrence is relatively low.[12] The release of a chemical agent or a weaponized biological agent in a crowded terminal or on a bus or train, or the intentional contamination of bulk food shipments with a chemical or biological agent, are particularly concerning possibilities. Protections from such events rely on early warning and indications of potential threats, and on informed and alert travelers and operators to report suspicious activities.

Priorities to address chemical and biological threats to public transportation are:

- Prepare and exercise contingency plans for chemical and biological agent releases;
- Improve information sharing regarding chemical and biological threats;
- Assure availability of response training for frontline employees;
- Identify detection capability gaps for potential research and development initiatives; and
- Sustain deterrence operations in public transportation venues such as Visible Intermodal Prevention and Response teams (VIPRs), technology applications, and similar state and local law enforcement initiatives.

G. Radiological and Nuclear Detection

DHS contributes to the security of global trade and travel in a variety of ways including integrating programs of multiple components to detect nuclear or other radioactive material out of regulatory control. The Domestic Nuclear Detection Office (DNDO) develops the Global Nuclear Detection Architecture, a framework to detect (through technical and non-technical means), analyze, and report on nuclear and other radioactive material out of regulatory control in aviation, maritime, and land transportation modes. DNDO researches, develops, acquires, and supports domestic detection capabilities while coordinating with other federal agencies that have primary responsibility to implement international efforts. DHS efforts across the supply chain include supporting Federal and state, local, tribal, and territorial (SLTT) organizations in their development of radiological and nuclear detection capabilities. Such assistance includes providing information resources and standardized and scalable templates, tools, processes, facilitation, and guidance on the development of strategic planning, concept of operations and standard operating procedures. DNDO's Assistance Program develops and delivers interior intermodal transportation and maritime radiological and nuclear detection programs, and the Mobile Detection Deployment Unit program. DNDO also coordinates Federal and SLTT radiological and nuclear detection program development through their Training and Exercises Programs, guidance documents, and technology solutions to increase capabilities to encounter and detect radiological and nuclear threats. DHS investigates the unlawful import and export of nuclear or other radioactive materials, technologies and capabilities, and detects and counters the importation and movement of weapons and materials into or within the United States.

Implementing the domestic portion of the Global Nuclear Detection Architecture requires the integrated efforts of Federal and SLTT responders for detection and interdiction. DNDO works with CBP to deploy radiation portal monitors and other radiation detection technologies to

[12] 2014 QHSR, p.19.

domestic seaports, land border crossings, airports of entry, and mail facilities. DNDO also procures thousands of personal radiation detectors, radiological isotope identification devices, and backpack detectors for CBP, USCG, and TSA officers to scan cars, trucks, vessels, cargo, and other items and conveyances.

H. Response and Recovery

Response and recovery following a terrorist attack involving transportation infrastructure and services requires a whole-of-community approach, including public and private sector owners and operators, as well as federal and SLTT governments. During incident response, transportation capabilities support evacuations, rescue, medical care, and incident management. After a terrorist attack, law enforcement authorities and emergency responders are responsible for preserving public safety, securing the crime scene, mitigating the threat, preserving evidence, and identifying and arresting the suspects. During recovery, transportation infrastructure and assets are essential for repair and restoration and for supplying community needs.

Federal policy for emergency preparedness and disaster management originates from Homeland Security Presidential Directive-5, "Management of Domestic Incidents," and Presidential Policy Directive 8, "National Preparedness." Under Presidential Policy Directive 8 the "Secretary of Homeland Security is responsible for coordinating the domestic all-hazards preparedness efforts of all executive departments and agencies, in consultation with State, local, tribal, and territorial governments, nongovernmental organizations, private-sector partners, and the general public; and for developing the national preparedness goal."[13] The National Response Framework and the National Disaster Recovery Framework describe the federal roles and responsibilities during the various stages of response and recovery. Coordination of all response and recovery actions during a disaster conforms to the National Incident Management System. In addition, numerous DHS and DOT component agencies have specific statutory responsibilities for response and recovery.

DHS and DOT share the responsibility for transportation emergency preparedness and response during declared emergencies or disasters. Specifically, DHS, through the Federal Emergency Management Agency, has the authority to provide grants for planning mass evacuations and to coordinate all disaster assistance provided by Federal and SLTT government agencies and private organizations, including precautionary evacuations. DOT's roles include reporting damage to transportation infrastructure, coordinating alternate transportation services, and coordinating the restoration and recovery of transportation infrastructure. Additionally, under the National Response Framework, DOT leads Emergency Support Function 1–Transportation– to coordinate transportation support for responses to declared disasters and emergencies.

Priority sector activities to improve response and recovery are:

- Enhance contingency plans for response to terrorist attacks in ports and High Threat Urban Areas (HTUAs);

[13] Presidential Policy Directive 8, National Preparedness, March 30, 2011, p. 4.

- Improve communication, coordination, and information sharing between Federal and SLTT law enforcement officials, first responders and emergency personnel, and private industry partners while managing the response to terrorist attacks;
- Promote participation in local security exercises to ensure public and private familiarity with plans, procedures, and capabilities; and,
- Incorporate structural design standards in transportation infrastructure to mitigate the consequences of attacks and improve recovery capabilities.

VI. Performance

A. Assessing National Transportation Security Performance

Federal, SLTT, and industry security partners will work jointly to develop a performance assessment regime to indicate progress in achieving priority outcomes. The measures of performance may be refined or revised to provide accurate and reliable indications of desired security outcomes for the 2015-2018 planning period. Generally, the strategic outcomes will be determined from performance data collected by government program managers or transportation operators responsible for implementing the security activities. The progress achieving prioritized, risk-based outcomes will be reported annually in accordance with 49 U.S.C. §114(s)(4)(C).

B. Performance Measures

The following table indicates TSA's external performance measures to show progress reducing terrorism risks, enhancing resilience to attacks, improving domain awareness, and protecting privacy, civil rights, civil liberties, and freedom of movement.

Table 1: Performance Measures

Outcome	Measure
Reduce security risk	• Number of annual VIPR operations to deter potential terrorist actions and enhance security at surface and aviation transportation facilities • Percent of Federal Air Marshal Service coverage targets met for each individual category of identified risk • Percent of indirect air carriers found to be compliant with TSA standard security programs
Improve domain awareness	• Percent of customers satisfied with the intelligence products provided
Protect privacy, civil rights, civil liberties, and the free movement of travelers and goods	• Percent of daily travelers eligible to receive expedited physical screening based on assessed low risk • Percent of policies, security directives, and executive ammendments receiving privacy, civil rights, and civil liberties review prior to release

VII. Roles and Responsibilities

A. Federal Government

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

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

B. SLTT Governments

SLTT government entities are the first to respond to terrorist incidents; consequently, SLTT governments are best positioned to address specific homeland security needs and to assume the lead for local preparedness. SLTT authorities assist the sector security managers to identify critical transportation assets; to determine security gaps and priorities; and to develop security, response, and recovery plans to protect those assets. Specific responsibilities of SLTT governments are further discussed in the National Infrastructure Protection Plan 2013.

C. Industry

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

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

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

VIII. Challenges and Path Forward

A. Evolving Threat Environment

The threat environment in transportation is constantly changing. Adversaries strive for ways to circumvent security measures. New methods and tactics to construct and deploy dangerous weapons are circulated on the Internet. New technologies, such as non-metallic weapons and Unmanned Aircraft Systems, challenge current screening, detection, and protection capabilities. Security officials will require advanced technological capabilities and continual training to detect and prevent emerging threats. Timely intelligence, an alert and knowledgeable workforce, and effective partnerships will sustain a security posture that deters terrorists. Security initiatives to deal with these risks must be weighed against the impacts on freedom of movement and commerce.

B. Resilience and System Recovery

Transportation systems serving travelers and commerce are complex intermodal networks. A terrorist attack involving transportation structures could have considerable long-term consequences for travel and commerce. A terrorist event could disrupt important transportation infrastructure, impact the local, regional, and national economies, and threaten public safety and security.

The survivability and sustainability of vital transportation services and infrastructure are important for the timely recovery of other sectors and services. Transportation industry and government entities responsible for security must collaborate to explore ways to build upon and exercise contingency response and recovery plans at the national, regional, and local levels. They must expand engagement initiatives to include other sectors to identify interdependencies, enhance preparedness for disasters, and expedite the recovery of the most essential transportation services.

C. Performance Assessments

Measuring the effectiveness of security initiatives across multiple government jurisdictions and diverse industries presents challenges for resource managers. However, in a constrained fiscal environment, managers require program measures that provide meaningful assessments of risk-reduction activities and the associated costs. Risk-reduction measurement is challenging for security managers due to difficulties of assessing baseline risk equitably across companies and across modes and of assessing effectiveness of specific initiatives. Even if reliable risk-reduction metrics were available for an initiative in one segment of the industry, comparing them to metrics in another segment is often not meaningful. Transportation security partners should jointly consider outcome performance measures during program development and, to the extent practicable, implement assessment methodologies to inform decisions.

D. Cybersecurity

Cyber threats represent a near- and long-term challenge because of rapidly growing digitization and networking of operational and business systems used in transportation. However, there is uncertainty about the capabilities and intent of adversaries to damage or disrupt transportation using cyber means. Consequently, many owners and operators are unsure of the level of risk and the type and extent of countermeasures they may need. Cyber-based control systems are networked wirelessly to remote sensors and operational components. These systems are often connected to the Internet and could be accessed through publicly available intrusion software. It is conceivable that terrorists could exploit the possibilities of conducting a cyber attack against aircraft or other transportation control systems.

The path forward to secure transportation systems from cyber attacks will require broad-based commitments to improve cybersecurity awareness and the use of best security practices by individuals, industries, and government agencies. Sector partners should work together to refine assessments of the cyber threats and vulnerabilities, and to assure timely sharing of cyber threat information with owners and operators. The partners should continue to implement the Transportation Systems Sector's Cybersecurity Strategy and support initiatives in the President's Executive order on Critical Infrastructure Cyber Security including implementation of the National Institute of Standards and Technology Cybersecurity Framework.

Acronym List

CBP	U.S. Customs and Border Protection
CSI	Container Security Initiative
Cyber EO	Critical Infrastructure Cybersecurity Executive Order
DHS	U.S. Department of Homeland Security
DNDO	Domestic Nuclear Detection Office
DOD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOJ	U.S. Department of Justice
DOS	U.S. Department of State
DOT	U.S. Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
GA	General Aviation
HMC	Highway and Motor Carrier
HSIN	Homeland Security Information Network
HTUA	High-Threat Urban Area
IED	Improvised Explosive Device
IOC	Interagency Operation Center
I-STEP	Intermodal Security Training and Exercise Program
ISPS	International Ship and Port Facility Security
IRTPA	Intelligence Reform and Terrorism Prevention Act
MSRAM	Maritime Security Risk Analysis Model
MSRO	Maritime Security and Response Operations

MTPR	Mass Transit and Passenger Rail
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
NSGSCS	National Strategy for Global Supply Chain Security
NSTS	National Strategy for Transportation Security
P&S	Postal and Shipping
R&D	Research and Development
RSSM	Rail Security Sensitive Materials
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
TSA	Transportation Security Administration
TSSRA	Transportation Sector Security Risk Assessment
TWIC	Transportation Worker Identification Credential
USPS	U.S. Postal Service
USCG	U.S. Coast Guard
VIPR	Visible Intermodal Prevention and Response
WMD	Weapon of Mass Destruction

Appendix A
2014 Aviation Security Plan

Homeland Security

Transportation Security Administration

I. Introduction

A. Overview

The aviation mode is comprised of General Aviation (GA), commercial airlines, commercial service airports, air cargo, and a myriad of aviation support activities within these components. The aviation community includes industry and infrastructure as well as numerous support services that require access to airport facilities and aircraft. The aircraft repair facilities, airport concessions, fuel services, ground maintenance and repair services, and food and drink vendors exemplify the extended community included in the aviation security network. Security for this extended aviation domain depends on effective partnerships and communication among governments (federal, state, local, tribal, territorial, and international government partners) and industry stakeholders, including aircraft, owners and operators, airport operators, shippers, industry associations, and passengers.[14]

Each year, there are approximately 640 million domestic and international aviation passengers and 1.5 billion checked and carry-on bags that are screened.[15] There are approximately 9,000 Foreign Private Charter and GA aircraft authorized in the U.S. airspace by the TSA Airspace Waiver Program.

Each day, airports process millions of passengers and tens of thousands of tons of cargo. There are an estimated 900,000 workers who perform duties in the secured areas of U.S. airports. The Aviation Transportation System is vitally important to U.S. prosperity and freedom; disruption of the critical infrastructure elements in the Air Domain could create ripple effects throughout the entire system. Terrorists regularly consider the aviation system and its elements as targets for attack, both direct and indirect.

[14] The Aviation Transportation System is defined as U.S. airspace, all manned and unmanned aircraft operating in that airspace, all U.S. aviation operators, airports, airfields, air navigation services, and related infrastructure, and all aviation-related industry.

[15] http://www.tsa.gov/sites/default/files/assets/pdf/tsabythenumbers_111714.pdf

Table 2: TSA-Regulated Components of the Aviation Mode[16][17]

Air Cargo	Air cargo includes property tendered for air transportation accounted for on an air waybill. All accompanied commercial courier consignments, whether or not accounted for on an air waybill, are also classified as cargo. The air cargo security operations serving the United States are made up of over 300 domestic and foreign air carriers, approximately 450 domestic commercial airports, numerous international airports in 104 countries (last points-of-departure), over 4,000 indirect air carriers (freight forwarders), and over a million world-wide shippers.
Commercial Airlines	Commercial airlines are those that engage in regularly scheduled passenger service or public charter operations, including domestic aircraft operators and foreign air carriers flying within, from, to, or over the United States.
Commercial Service Airports	Commercial airports are defined as airports with regularly scheduled commercial passenger service or public charter operations. There are approximately 450 airports in the United States that are staffed with TSA security workforce and that have Airport Security Programs.[18]
Flight Schools	Flight schools include any pilot school, flight training center, air carrier flight training facility, flight instructor, or any other person or entity that provides instruction in the operation of any aircraft or aircraft simulator.
General Aviation	The GA mode includes any of approximately 19,360 airports, heliports, and landing strips where GA aircraft operate, including commercial airports as described above. It is estimated that there are more than 5,100 public-use GA airports in the United States. GA aircraft are all aircraft except those engaged in military or regularly scheduled commercial passenger operations. GA includes diverse industries and operations, including private-use recreational aircraft, business jets, and emergency medical helicopters. GA accounts for approximately 77 percent of all flights in the United States.
Repair Stations	Foreign and domestic repair stations inspect, repair, replace or overhaul aviation articles including airframes, propellers and radios among others.

1. Purpose

The purpose of the Aviation Security Plan is to address high priority security risks including threats, vulnerabilities, and consequences for aviation. The Aviation Security Plan provides a strategic approach to securing U.S. aviation from terrorist attacks. It advances the strategic goals of the NSTS by identifying objectives and activities. It also fulfills the requirement of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, as amended, and builds upon, complements, and augments the broad principles of the 2007 National Strategy for Aviation Security and its seven supporting plans.[19]

[16] 2010 Transportation Systems Sector-Specific Plan

[17] Other Federal agencies with regulatory authority related to aviation may describe or define categories of the aviation mode differently from the categories described by TSA for the purposes of this report.

[18] Eighteen Commercial Airports participate in the Screening Partnership Program (SPP) program http://www.tsa.gov/stakeholders/screening-partnership-program

[19] Per the National Security Presidential Directive 47/Homeland Security Presidential Directive 16, the three broad principles provide overarching guidance to the National Strategy for Aviation Security, and its objectives and actions: The Nation must use the full range of its assets and capabilities to prevent the Air Domain from being

2. Risk Profile and High-Risk Scenarios[20]

The risk profile for the aviation mode of transportation includes threats from domestic actors, but is dominated by international and transnational terrorism. Aviation security relies on threat intelligence and risk assessments to determine risk-based priorities. In addition, aviation analysts review data from security inspections, exercises, and incident reports to identify vulnerabilities and develop mitigation strategies. Risks to aviation, domestic and international, remain high given the expressed intentions of terrorists, their persistent attempts to thwart security and target aviation, and the perceived fiscal and human consequences of a successful attack.

Aviation is increasingly dependent on cyber systems for aircraft operations, air and ground traffic control, passenger ticketing, and baggage and cargo tracking. Although no attacks on cyber systems serving the aviation industry have been attributed to terrorists, a determined adversary could attempt to identify and exploit vulnerabilities to attempt to cause considerable disruption of air travel. Frequent reports of attacks and intrusions into sensitive data or control systems serving other sectors indicate the potential for substantial cyber-related security and safety risks to aviation.

The following risk profiles and high-risk scenarios, informed by the Transportation Sector Security Risk Assessment and other intelligence analyses and assessments, provide a basis for risk-based aviation security priorities.

Commercial Airlines Risk Profile: The risk of terrorists attacking or using commercial aircraft includes threats of hijacking, the introduction of explosives or other weapons into the aircraft, and attacks using standoff weapons, such as Man Portable Air Defense Systems. While security measures have significantly reduced aviation risks, aircraft-related security risks remain elevated due to persistent attempts by terrorists to thwart security measures. Aircraft are also vulnerable to standoff weapons attack, especially at international last points of departure airports in high-risk locations.

Commercial Airlines High-Risk Scenarios: There are three main high-risk scenarios. First, commercial aircraft may be used as Weapons of Mass Destruction (WMD) if commandeered or hijacked; second, commercial aircraft may be attacked by introducing explosives onto aircraft by persons, baggage, or cargo; and third, commercial aircraft may be attacked using standoff weapons.

Commercial Airports Risk Profile: Commercial airports are multi-modal hubs characterized by efficient and convenient access to arrival and departure areas of the terminals. The greatest risks for airports are related to attacks in publicly accessible areas. Explosives may be introduced in baggage, on persons, or by vehicles. Secure areas of airports, though tightly

---

exploited by terrorist groups, hostile nation-states, and criminals who intend to commit acts against the United States, its people, its infrastructure, and its other interests. The Nation must ensure the safe and efficient use of the Air Domain. The Nation must continue to facilitate travel and commerce.

[20] Risk Profiles and Scenarios sources include TSSRA and TSA aviation assessments.

controlled, are vulnerable to forcible intrusion by individuals or small tactical units that could breach checkpoints or perimeter barriers. Terrorist attacks may also be facilitated by insiders, wittingly or unwittingly, providing information or access needed to execute the attack.

Commercial Airports High-Risk Scenarios: The primary risk scenario for commercial airports—domestic and foreign—is an attack using one or more IEDs or assaults by lone or small unit attackers (e.g., at airport lobbies and other passenger areas). Most probable scenarios involve IEDs delivered by vehicles, in baggage, or by a suicide bomber.

Air Cargo Risk Profile: Air cargo risks are magnified by the vast number and diversity of shippers, cargo handlers, and carriers in the global supply chain. Air cargo is transported on a wide range of aircraft—from large express consignment carriers that operate complex sorting operations at major hubs to small regional carriers that move high-value cargo or serve rural areas. Terrorists may attempt to ship weapons and explosives as supplies for attacks or, in an extreme case, transport WMD into the United States. Cargo shipments on passenger aircraft increase security risks, particularly for flights originating in areas of conflict.

Air Cargo High-Risk Scenarios: Threat and risk assessments identify several primary risk areas in the air cargo industry. Air cargo may be used to deploy a WMD or to transport IEDs to attack passenger aircraft.

General Aviation Risk Profile: The terrorist threats to GA operations and facilities are understandably similar to those for commercial aviation and federalized airports. Generally, GA facilities are considered to have a lesser risk of terrorist attack than commercial aviation facilities due to the smaller size and limited volume of travelers. However, GA aircraft are vulnerable to being used by terrorists for travel, logistics, or operations. As vulnerabilities associated with commercial passenger operations are mitigated, it is believed that terrorists may view GA as more vulnerable and thus attractive targets.

General Aviation High-Risk Scenarios: Terrorists could enter the country on small aircraft to avoid screening at departure and entry points. Small aircraft could be commandeered for use in an attack. Dangerous materials could be shipped into or within the United States for subsequent use by terrorists. GA aircraft could be used as weapons or to deliver weapons. Fast GA aircraft with transcontinental range may be of particular interest to terrorists planning to attack critical infrastructure.

B. Risk-Based Priorities

The following risk-based priorities for the aviation mode are derived from modal threat assessments and national strategies such as the 2014 DHS Quadrennial Homeland Security Review and the National Strategy for Aviation Security:

- Protect the Aviation Transportation System from catastrophic terrorist attack;
- Advance risk-informed, intelligence-driven approaches to aviation security;
- Protect against cyber threats to the aviation domain;

- Maximize shared air domain awareness of domestic and international threats with the Intelligence Community, critical infrastructure partners, and aviation sector industry;
- Improve international partnerships and security cooperation to increase aviation security worldwide and prevent terrorist attacks;
- Enhance the resilience of the Aviation Transportation System through response and recovery planning, training, and exercises;
- Protect the privacy, civil liberties, and civil rights of travelers; and,
- Leverage technologies to improve explosives detection and screening capabilities, and to enhance security threat assessments and watch list matching.

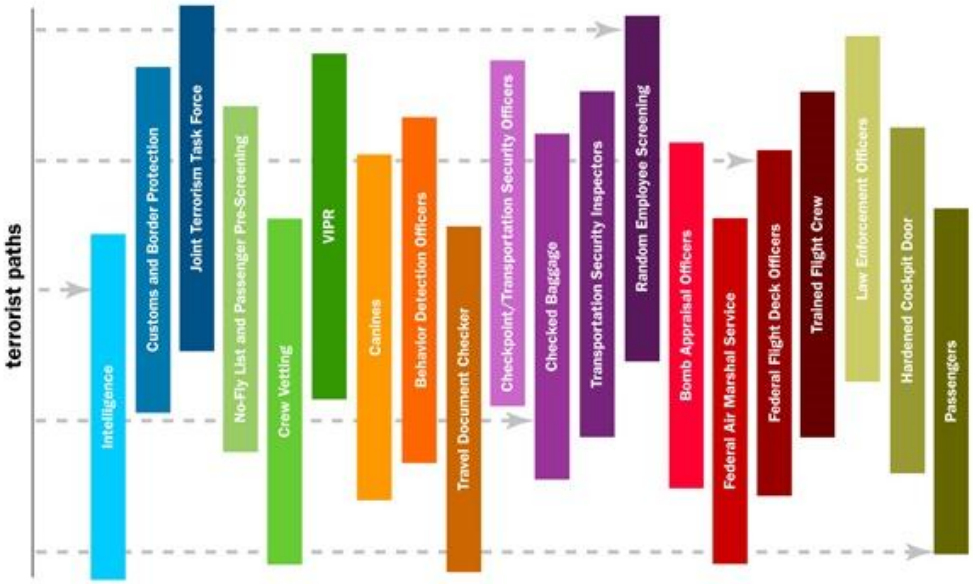
II. Programming Priorities

A. Description

The aviation mode develops strategies collaboratively to reduce security risks. The key is the shared awareness and recognition by public and private sector entities of their common interests in protecting aviation resources (e.g., people, aircraft, cargo, and infrastructure) from terrorist attacks.

The United States uses layers of security to ensure the traveling public and the Nation's transportation systems are protected. TSA is most often associated with the airport checkpoints. Checkpoints are just one layer of security among the many counterterrorism measures in place. Each countermeasure, represented by the bars in Figure 1, is intended to deter, detect, and prevent one or more paths terrorists might take to execute an attack. In combination, the layers enhance security, creating a much stronger and protected transportation system.

Figure 1: Layers of U.S. Aviation Security



The application of Risk-Based Security has become a foundational security principle in all modes of transportation. Risk-Based Security is a shift from a "one size fits all" philosophy of applying security measures to an intelligence driven and risk informed approach, with finite security resources being allocated relative to the community's knowledge of threat and vulnerabilities. Through Risk-Based Security, more security resources are allocated against potential known and unknown threats, with fewer security resources allocated to screening of persons and objects that are known and trusted. The community further reduces consequences by enhancing the resilience of aviation infrastructure and operations.

B. Goals, Objectives and Activities

Section B lists the Aviation Security goals and the objectives based on the Transportation System Sector's Risk-Based Priorities. This section also highlights the corresponding activities that encompass the whole-of-government approach to national aviation security.

Table 3: Aviation Security Goals

NSTS Goal 1: Manage risks to aviation transportation systems from terrorist attack and enhance system resilience	
Objective 1: Improve physical and cyber security of aviation critical infrastructure	
Activity 1	Enhance security measures (e.g., VIPR, access controls, and physical security) to protect critical National Airspace System infrastructure (DOT/FAA, DHS/TSA, DOJ/FBI, industry)
Activity 2	Apply a risk-based, layered approach, consistent with unity of effort principles to facilitate the movement of people and commerce while focusing security resources on higher-risk travelers, workers, facilities, aircraft, cargo, and baggage (DOJ/FBI, DOS, DHS/CBP/TSA)
Activity 3	Engage aviation security partners to encourage voluntary implementation of the National Institute of Standards and Technology Cybersecurity Framework
Objective 2: Improve preparedness and response capabilities to deter, detect, respond, and recover from terrorist attacks throughout the aviation community	
Activity 1	Develop a response planning and exercise regime that aligns and coordinates government and industry plans and air operations (DOT/FAA, DHS/TSA, DOJ/FBI, DOS, DOD, industry)
Objective 3: Improve international aviation security capacity	
Activity 1	Harmonize international security policies, procedures, and training to be equivalent to those of the United States through coordination and outreach in international forums (DOE, DOJ/FBI, DHS/CBP /TSA/DNDO, DOT/FAA, DOS)
Activity 2	Increase the effectiveness and efficiency of the passenger and baggage screening internationally, e.g., Preclearance airports, capacity development, and Trusted Traveler programs (DHS/CBP/TSA, DOS)
Objective 4: Increase security technology capability to respond to known and emerging threats	
Activity 1	Improve industry participation in the R&D process (DOT, DHS/TSA, R&D community, industry)
Activity 2	Improve aviation security threat detection and screening capabilities (e.g., on-board aircraft detection, ground-based detection, Explosives Detection System, Explosives Trace Detectors, closed circuit television, motion detectors, auto alarms, and biometric identifiers) (DOT, DHS/TSA, R&D community, industry)

NSTS Goal 2: Enhance effective air domain awareness of transportation systems and threats[21]	
Objective 1: Improve quality and timeliness of intelligence and information products for government, industry, and public awareness	
Activity 1	Advocate the aviation security community's support for public awareness (e.g., See Something, Say Something) (DHS, industry)
Activity 2	Improve air domain awareness information processing tools and analytic capabilities
Activity 3	Improve reporting of suspicious security activities (e.g., Nationwide Suspicious Activity Reporting Initiative" campaign, and GA Watch program) (DHS, industry)
Activity 4	Enhance development of high-risk scenarios in risk assessments to improve awareness of threats, vulnerabilities, and countermeasures (e.g., TSSRA) (DHS, DOJ/FBI, Office of Director of National Intelligence)
Objective 2: Improve collaboration among private sector and government agencies regarding intelligence and information sharing (DHS, DOT, DOJ/FBI, Fusion Centers	
Activity 1	In coordination with interagency initiatives, build effective processes for enhanced collaboration across federal, state, and local operations centers and with international partners
Activity 2	Increase discussion of strategic priorities at open-forum meetings of aviation security stakeholders to address strategic priorities (e.g., Aviation Security Advisory Committee, Aviation Government and Sector Coordinating Councils, and periodic industry association meetings)
Activity 3	Ensure timely sharing of actionable threat information among partners through regular classified intelligence briefings
Activity 4	Develop air domain intelligence integration and analysis of physical and cyber threats among the Intelligence Community, critical infrastructure partners, and the aviation industry

NSTS Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce	
Objective 1: Reduce the potential negative impact of security policies and activities to privacy, civil rights, and civil liberties	
Activity 1	Ensure aviation policies, procedures and technologies are reviewed by designated privacy and civil rights officials (e.g., TSA Pre✓®) (DHS/Office of the General Counsel/TSA, Office of Management and Budget, DoD, White House Office of Information and Regulatory Affairs, industry)
Activity 2	Ensure strict disclosure controls on all personally identifiable information to protect it from misuse or unauthorized disclosure (e.g., Privacy Impact Assessment for the Aircraft Systems, such as Unmanned Aircraft Systems, and Secure Flight) (DOJ/FBI, DOS, DHS/CBP/TSA, DOT/FAA)
Objective 2: Apply risk-based security approach to supply chain and traveler movements	
Activity 1	Improve traveler experience for low-risk travelers using risk-based security and Trusted Traveler Programs, such as NEXUS, Global Entry, SENTRI, and FAST (DHS/TSA/CBP)
Activity 2	Improve delivery times for air cargo and wait times for travelers, and monitor performance against standards (DHS/TSA/CBP)
Activity 3	Improve efficiencies of security measures for passengers and cargo such as Global Entry, TSA Pre✓®, Air Cargo Advanced Screening, and National Cargo Security Program Recognition (DHS/TSA/CBP/USCG)

[21] Source: Air Domain Surveillance Intelligence Integration Plan

III. Challenges, Opportunities, and Path Forward

Table 4: Aviation Challenges, Opportunities, and Path Forward

Challenges or Opportunities	Path Forward
The persistence and adaptability of terrorists: Of particular concern is the growth of terrorist groups and the possibility that terrorists will seek to surpass the terrible toll of 9/11	• Government agencies and the aviation industry will continue to work together to address security in the most effective and efficient way, while protecting privacy and preserving civil liberties and civil rights. The success of the layered security strategy depends on rapid recognition and communication of threats to responsible government and industry security officials. Security partners should have a common awareness of the air domain in steady-state and during incidents to validate and enhance early detection of threats and direct appropriate responses. Government agencies in particular must continue work to eliminate the barriers that create information silos and to identify technologies to improve domain awareness. • The Intelligence Community will enhance access to sources to improve its ability to identify current and emerging terrorist threats and tactics. Aviation security will require continual investment to improve detection capabilities for current and future threats and to minimize the intrusiveness, delays, and inconvenience of security measures on commerce and travel. New security technology should be developed, tested, and deployed to increase the effectiveness of intelligence programs. • Government and industry must be vigilant to indications of terrorists' intents and capabilities to exploit cyberspace and must develop technologies to detect, defend against, and respond to attacks.
New and innovative weapons, tactics, and delivery methods: The greatest threat to aviation security remains explosives, especially non-metallic IEDs. Terrorist methods will involve more sophisticated, non-metallic IEDs, and they will seek to develop and/or acquire weapons with greater lethality, including WMD.	
The threat of domestic terrorism is increasing and difficult to interdict: The threat includes so-called "lone wolf" and small team assailants. The public areas of the nation's airports are open and afford attackers access to populated assembly areas for ticketing, baggage pick-up, or screening.	
Use of Unmanned Aircraft Systems: Unmanned Aircraft Systems, often referred to as drones, used for business, research, and recreation, are opening a broad new avenue for delivery of weapons by terrorists. Unmanned Aircraft Systems are easily obtained and could be used to deliver a lethal payload of explosives or chemical, biological, or radiological/nuclear agents with little opportunity for interdiction.	

Appendix B
2014 Maritime Security Plan

Homeland Security

Transportation Security Administration

I. Introduction

Our Nation's maritime critical infrastructure continues to face complex and evolving challenges. Maritime risks stem from a mix of naturally occurring and man-made hazards and threats, including terrorist attacks (both domestic and international), cyber threats, catastrophic accidents, rising sea levels, natural disasters, and other emergencies. The 2014 Maritime Security Plan addresses the security of maritime assets that must be protected from terrorist attacks.

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

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

A. Overview

The MTS in the United States is a geographically, physically, and operationally diverse network of maritime and shore side operations consisting of 25,000 miles of navigable channels, 238 locks at 192 locations, and over 3,700 marine terminals. Waterborne cargo and associated activities contribute more than $649 billion annually to the U.S. Gross Domestic Product, and sustain more than 13 million American jobs. Over 75 percent by weight of international trade enters or leaves the United States by ship.[22] The National Strategy for Maritime Security (NSMS) and its supporting plans, affirmed by the President in August 2012, establishes the U.S. policy to to enhance the security of and protect U.S. interests in the Maritime Domain. This includes activities to prevent terrorist attacks in the Maritime Domain, and enhance U.S. national security and homeland security by protecting U.S. population centers, critical infrastructure, borders, harbors, ports, and coastal approaches in the Maritime Domain

1. Purpose

The Maritime Security Plan meets the maritime modal plan requirement of the National Strategy for Transportation Security required by 49 U.S.C. §114(s). Along with NSMS, it presents risk-based priorities and activities to protect the MTS from terrorism and to enhance system recovery following a terrorist incident.

[22] Federal Highway Administration, Freight Facts and Figures 2013. Available at http://ops.fhwa.dot.gov/freight/freight_analysis/nat_freight_stats/docs/13factsfigures/figure2_05.htm#metric

2. Risk Profile and High-Risk Scenarios[23]

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

- **WMD:** The extreme consequences of a WMD event make it a significant risk. A comprehensive set of threat identification and detection capabilities is required to reduce the threat of WMD transfer. Vessels under 300 gross tons (considered small vessels) could by targeted by terrorists or saboteurs as opportunities to smuggle dangerous weapons, including WMDs, into the United States.
- **Terrorist Transfer:** The risk of terrorist transfer by a vessel of any size into the United States is a serious concern. The deadly December 2008 attacks in Mumbai, India, highlighted the threats posed by small vessels used to convey terrorists into or through any nation's maritime domain. The probability of such an attack may increase with the expected growth in the movement of passengers, vessels, and hazardous cargo.
- **Small Vessel Terror Attack:** Millions of small commercial and recreational vessels operate on U.S. waterways. Vessels under 300 gross tons are not required to carry electronic identification devices, make advance notices of arrival, or otherwise alert authorities to their whereabouts; thus they constitute a major maritime domain awareness gap. Consequently, a more likely threat is the use of a Waterborne IED on a small vessel to attack a ship or waterfront facility. In addition, small vessels may be used to conduct standoff attacks. In November 2005, pirates in rigid hull inflatable boats used rocket-propelled grenades and automatic weapons to attack a cruise ship off the coast of Somalia. It is technically feasible to launch a ballistic missile from a ship as small as 200 tons against the United States. Many U.S. airports are built in the vicinity of navigable waters.

Cyber Risk: Both cyber exploitation by malicious actors, including terrorists, as well as unintentional incidents due to operator error or accidental software/hardware failures, pose a risk to maritime transportation. Maritime operations rely on cyber-based technologies for communications, navigation, positioning, tracking, cargo handling and stowage, and shipboard control systems. These systems are often networked with shore-based systems. Cyber attacks targeting the systems on which vessels and port operations rely are unlikely to cause significant disruption of national or regional maritime operations due to the overall resilience of the commercial port and maritime industries. However, localized impacts such as port delays and interrupted delivery schedules could occur.

[23] Sources include the USCG's report to Congress *Threat of Terrorism to U.S. Ports and Vessels in 2013.*

Especially Hazardous Cargo Release: Especially Hazardous Cargoes are transported, transferred, and stored in numerous ports and waterways, particularly the Gulf Coast region and the Western Rivers.[24] Due to Especially Hazardous Cargo's chemical and physical properties, their release in the MTS could threaten nearby populations, cause significant damage to the environment, and disrupt commerce.

B. Risk-Based Priorities

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

- Implement risk-based security planning and operations to reduce the terrorism risk;
- Increase enforcement of Maritime Security Regimes;
- Enhance Maritime Domain Awareness;
- Conduct Maritime Security and Response Operations; and
- Enhance cyber safety, security and resilience for MTS owners/operators.

[24] Especially Hazardous Cargo means anhydrous ammonia, ammonium nitrate, chlorine, liquefied natural gas, liquefied petroleum gas, and any other substance, material, or group or class of material, in a particular amount and form that the Secretary determines by regulation poses a significant risk of creating a transportation security incident while being transported in maritime commerce.

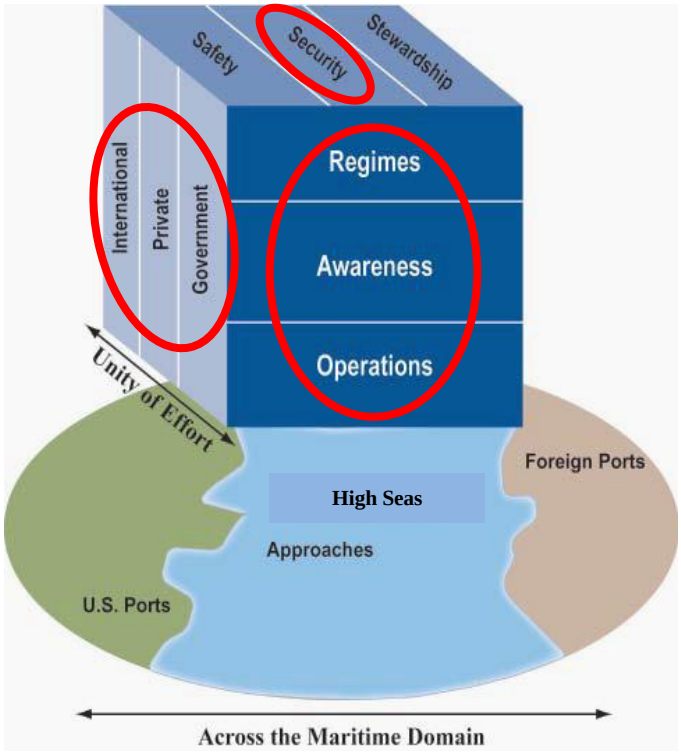
II. Programming Priorities

A. Risk Reduction Programs and Activities

A variety of risk mitigation activities is employed to address scenarios across the risk spectrum. USCG and its federal and international partners have extensive statutory authority, presence, command and control capability, and experience in maritime safety and security. USCG leads the maritime community's collaborative efforts in its legislatively mandated Ports, Waterways and Coastal Security mission to prevent, protect against, respond to, and recover from terrorist attacks, sabotage, espionage, or subversive acts in the maritime domain.[25] Ports, Waterways and Coastal Security includes the establishment and oversight of Maritime Security Regimes, employment of Maritime Domain Awareness, and the execution of Maritime Security and Response Operations (MSRO) activities.

Ports, Waterways and Coastal Security uses a layered security strategy that "pushes out the borders" in an effort to reduce the threat to maritime infrastructure. This approach maximizes early warning of maritime-related threats originating from foreign ports and routed through the high seas prior to entering the waterways of the Nation. The layered approach employs a maritime governance model that shares responsibilities with many partners – domestic and international.

Maritime Security Regimes comprise the rules and protocols that enhance collaboration on maritime infrastructure resilience and recovery planning, exercises, and operations. This element of layered security implements domestic and international statutes, regulations, and agreements that coordinate partnerships and establish maritime security standards.



- The Maritime Transportation Security Act (MTSA) requires USCG to collaborate with private sector ships and port facilities to assess their vulnerabilities and develop measures to reduce them. MTSA also requires the identification of threats to maritime critical assets and infrastructure. USCG periodically assesses the effectiveness of anti-terrorism measures in both U.S. and foreign ports and takes action in cases where effective anti-terrorism measures are not in place. Commensurate with the provisions of the MTSA, USCG supported the International Maritime

[25] Homeland Security Act of 2002 and Title 14 U.S.C.

Organization in the development of an international code, designated the International Ship and Port Facility Security (ISPS) Code. The ISPS Code contains security-related requirements for all signatory governments, port authorities and shipping companies, together with a series of guidelines and recommendations for meeting those requirements. USCG's International Port Security Program engages with foreign governments and visits foreign ports to assess their compliance with the ISPS Code and to improve security through dialogue and targeted capacity building.

- The Container Security Initiative (CSI) is part of the CBP layered cargo security strategy. CSI addresses the threat to border security and global trade posed by the potential terrorist use of a maritime container. CBP executes the program by deploying multidisciplinary teams to foreign seaports. These teams target and examine high-risk cargo before it is placed on vessels bound for the United States. This process enables greater security through collaboration. CSI operates in over 55 ports worldwide. Based on strategically determined locations, maritime cargo imported into our Nation is subject to the CSI program including Non-Intrusive Inspection and Radiation Portal Monitor technology to identify contraband and weapons of mass effect.
- SAFEPORT: The Maritime Administration supports law enforcement and border security with the SafePort program. The operational concept of SafePort is to remove a "suspect container" by sailing one of the Maritime Administration's crane ships to meet with the vessel offshore and removing the container for further inspection. The Maritime Administration works within a joint command structure among USCG, DHS, the FBI, and other relevant agencies to facilitate SafePort.
- TSA's Transportation Worker Identification Credential (TWIC) regulations are implemented in the maritime domain for workers requiring unescorted access to secure areas of port facilities, Outer Continental Shelf facilities, and vessels regulated under the MTSA. TSA and USCG implement the TWIC program to help ensure only vetted individuals have access to secure areas. The TWIC program furthers the multi-layered approach to the safeguarding of the MTS and port critical infrastructure.

Maritime Domain Awareness is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment. The maritime domain is defined as all areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. Together, maritime security regimes and Maritime Domain Awareness inform security decisions regarding trends, anomalies, and activities that threaten U.S. interests. Sharing information in the maritime environment regarding vessels, activities, and operators is a critical component in the DHS mission success. Through a number of operational, technological, programmatic, and policy-related initiatives, DHS leads efforts to improve information sharing among departmental components and other federal, SLTT, international, and private sector partners.

- The National Maritime Intelligence Center is an interagency facility housing the Director of National Intelligence's National Maritime Information Integration Office; the U.S. Navy's Office of Naval Intelligence; and USCG's Intelligence Coordination Center. Collectively, this center and other federal information sharing mechanisms allow for the synthesis of real-time maritime information and intelligence regarding threats to U.S.

ports and vessels. Other information hubs that support maritime transportation security include USCG Maritime Intelligence Fusion Centers, the CBP National Targeting Center, and the DHS National Infrastructure Coordinating Center.

- Interagency Operation Centers (IOC) have been established at 35 large ports (per requirements of the 2006 SAFE Port Act) by USCG and its partners. A port's IOC is the foundation of a coalition of federal and SLTT government first responders that conduct risk-based operational planning for improved port security. The IOC underpins the framework necessary to synchronize single-agency mission planning with a more holistic interagency operational planning and monitoring effort. The IOCs at all major ports are enhanced by a Federal Maritime Operations Coordination Plan. The DHS Science and Technology Directorate aids IOC development by evaluating sensor and information sharing technologies to improve data sharing among port partners.

MSRO is the third element of the Ports, Waterways and Coastal Security mission set. The MSRO mission encompasses integrated and layered security operations to deny the use or exploitation of the maritime domain by criminal or hostile actors and to deter or defeat attacks by terrorists using small vessels. MSRO activities include:

- Waterborne, shoreside, and aerial patrols;
- High-risk vessel escorts;
- Threat response;
- Incident recovery operations;
- DoD Military Outload security support;
- Enforcement of fixed and moving security zones;
- Control of port access, waterfront activities, and vessel movements;
- Waterborne security boardings; and
- Focused regional surge operations.

Another dimension of the layered maritime security system performed under MSRO is multi-mission offshore operations. USCG and CBP vessels and aircraft, supported by DoD and international partners, maintain continuous presence at-sea to provide domain awareness and interdiction and enforcement capabilities. USCG has personnel trained and equipped to conduct Short Notice Maritime Response operations in high threat/high risk environments including responding to chemical, biological, radiological, nuclear, or high-yield explosive threats. Short Notice Maritime Responses operations include underwater port security, canine explosives detection, vertical (helicopter) insertion, and opposed boarding tactics. MSRO assets are deployed for terrorism prevention and response based on intelligence and risk-informed contingency planning for potential terrorist courses of action within the maritime domain.

B. Goals, Objectives and Activities

Table 5: Maritime Security Goals

Goal 1: Manage risks to transportation systems from terrorist attack and enhance system resilience	
Objective 1: Utilize risk-based security planning and operations to reduce the terrorism risk to the MTS	
Objective 2: Reduce security vulnerabilities and improve preparedness throughout the MTS	
Activity 1	Expand cybersecurity protections in all segments of the MTS using the National Institute of Standards and Technology Framework
Activity 2	Improve compliance at MTSA facilities through risk-based adjustment of enforcement operations tempo
Activity 3	Improve interoperability of federal and SLTT response teams in Maritime Security and Response Operations
Activity 4	Employ MSRAM and other risk assessment and analysis tools to refine the estimates of MSRO activities' risk reduction benefits and use these estimates to inform the execution of MSRO activities in U.S. ports
Activity 5	Improve ISPS Code implementation in foreign ports that send ships to the United States
Activity 6	Explore potential use of floating security barriers at critical infrastructure and key resources to provide deterrence and resilience
Activity 7	Conduct random, unpredictable operations, such as VIPR deployments, to mitigate terrorist risk to the traveling public and maritime infrastructure

Goal 2: Enhance effective domain awareness of maritime transportation systems and threats	
Objective 1: Improve the security, resilience, and regulatory (federal/SLTT) information sharing process throughout the MTS community	
Objective 2: Improve MTS stakeholder participation in the risk management process for security and resilience prioritization and programming	
Activity 1	Enhance Maritime Domain Awareness tools and capabilities
Activity 2	Improve effectiveness of port exercise programs by designing exercise objectives and events based on analysis of MSRAM risk data
Activity 3	Enhance resilience of cyber systems through expanded exercises and assessments

Goal 3: Safeguard privacy, civil liberties, and civil rights; and the movement of people and commerce	
Objective 1: Collaborate with international partners to increase the resilience of key foreign ports and foreign infrastructure critical to the MTS and global supply chain	
Activity 1	Enhance joint CBP/USCG practices and use of the Maritime Infrastructure Recovery Program for the expeditious recovery of trade
Activity 2	Enhance preparedness of ports through the Area Maritime Security Committee Improvement Process

III. Challenges, Opportunities, and Path Forward

The main challenge to MTS security and resilience is the complex mix of man-made and naturally occurring threats, including terrorist attacks, accidents, natural disasters, and other emergencies. Maritime border activities include the movement of thousands of deep draft vessels intermingled with millions of recreational boats, fishing vessels, research vessels, workboats, and military vessels. The detection of threats is challenging due to the expansiveness of the maritime domain. Throughout the maritime domain terrorists have opportunities to conceal their activities and choose from multiple targets. These challenges require an informed, whole-of-nation approach to protect our ports, waterways, and waterfront facilities.

Ensure a Risk-Informed Investment of Fiscal Resources: A challenging fiscal environment makes resource planning extremely difficult for government and the private sector. To address this challenge government and industry will need to work together to identify efficiencies and eliminate redundancies. To meet priority security needs, the maritime community will require enhanced domain awareness capabilities and improved tools for risk-informed decision-making.

Determine the Threat of Maritime Terrorism: Protection from terrorist attacks requires effective deterrence, early detection, and timely interdiction. However, the magnitude of the maritime domain and the volume of maritime commerce and travel provide terrorists with ample opportunities to attack. Improved intelligence and threat communication, effective suspicious incident reporting and resolution, enhanced information management, and improved risk-based threat detection are capabilities that require continued investment. USCG conducts an annual assessment of threats to the MTS. CBP's layered approach to cargo security, including CSI, identifies the potential threat of a WMD in a container being introduced into one of our Nation's ports. DNDO coordinates programs among partners from federal, SLTT, and foreign governments as well as the private sector to detect nuclear and other radioactive material in shipments arriving on vessels. Another serious challenge is determining the intent of vessel operators, especially those operating small boats, in crowded ports and approaches. Implementing the DHS Small Vessel Security Strategy remains a challenge due, in part, to limited resources for coordinating the protection operations of federal and SLTT marine patrols.

Enhance Cybersecurity for Maritime Critical Infrastructure: For more than two centuries, oceans have served to insulate the United States from many threats. They have served as a buffer, affording time to identify and deter an attack. In today's cyber environment, however, ocean barriers provide much less protection Despite recent advances in intelligence and computer/network countermeasures, nefarious actors' exploitation of the expansive cyber domain as an attack vector for the nation's maritime critical infrastructure remains a significant challenge. Threats to the maritime information technology infrastructure can come from a wide array of sources. For example, advanced persistent threats – where adversaries possess sophisticated levels of expertise and significant resources to pursue their objectives – pose an increasing risk. Threat sources include corrupt employees, criminal groups, hackers, and terrorists. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary or political gain or mischief, among other things.

Balance Military Contingency Support and MTS Security: In the near term, the United States is demobilizing from the current major Overseas Contingency Operation in Afghanistan. Over the long term, the United States can expect to mobilize and then demobilize for other military crises or national emergencies overseas. The deployment and redeployment of forces in future mobilization or national emergency events may trigger increased security for domestic military outload facilities and vessel operations. Any long-term military outload and surge in related vessel movements may warrant sustained high priority USCG, other federal, and SLTT protective escorts and point defense operations, which may place constraints upon the Nation's capacity to provide adequate security for the MTS.

Appendix C
2014 Surface Security Plans

Homeland Security

Transportation Security Administration

Surface Security Plans Introduction

The Surface Security Plans appendix of the National Strategy for Transportation Security contains the security plans for the ground modes of the Nation's transportation system. The modal security plans fulfill a requirement of the IRTPA of 2004 (as amended), to address the threats, vulnerabilities, and consequences for transportation modal assets that could be at risk from attack or disruption by terrorists or other hostile forces.[26] The Surface Security Plan includes modal plans for Freight Rail, Mass Transit and Passenger Rail, Highway and Motor Carrier, and Pipelines.

[26] 49 U.S.C. §114(s)(1)(B) and §114(s)(3)(A)

Freight Rail Security Plan

I. Introduction

A. Overview

The Freight Rail Security Plan sets priorities for strategic preparedness, collaboratively developed by government officials and industry stakeholders, to enhance and sustain capabilities for protection of the Nation's railroad system from terrorist attack. The Freight Rail Security Plan meets the modal security planning requirements defined by the IRTPA of 2004 (as amended).

1. Risk Profile

The freight rail network is a vital part of the national economy, playing a key role in the global supply chain for both raw materials and finished goods. Freight rail is an important carrier for intermodal containers, often delivering imported goods to inland ports and domestic products across regions and states. As such, many sectors of the economy depend on freight railroads as a primary transporter, whether for commodities necessary to their operations, or for products and resources bound for domestic and international markets. Disruptions to critical nodes of the national rail network could have adverse impacts on efficient flows of these varied materials, with the prospect of consequential adverse effects on the supply chain in multiple sectors of the economy.

Freight railroads also host passenger rail operations over a significant portion of the Nation. The segments of the freight rail network that have passenger and commuter rail sharing the same tracks are exposed to additional risk from attacks directed at passenger operations.

Consistent with the sector-wide effort to improve the security of cyber systems on which transportation relies, the mode will manage cybersecurity risks by improving system protections and resiliency, facilitating security awareness, and promoting voluntary, collaborative, and sustainable community action as described in EO 13636 *Improving Critical Infrastructure Cybersecurity*.

2. Risk Scenarios[27]

The Freight Rail mode's primary risk scenarios include attacks using IEDs to cause the catastrophic release of hazardous rail cargos and attacks that would result in the loss of critical transportation system infrastructure, causing a disruption of the freight rail network or loss of life.

[27] TSSRA 3.0 2014

B. Risk-based Priorities

- **Security Planning**: Sustain effective security plans through the identification of threats, assessment of vulnerabilities, and evaluation of potential consequences.
- **Security Training**: Provide effective training for frontline employees in security-sensitive positions.
- **Security Exercises**: Conduct effective exercises employing realistic threat scenarios that evaluate and identify opportunities to improve security and resilience.
- **Intelligence and Security Information Sharing**: Maintain and enhance the means and mechanisms for sharing information and intelligence between industry and government.
- **Risk Reduction**: Maintain the operational procedures for reducing the risk associated with the rail transportation of security-sensitive materials.
- **Community Outreach**: Engage with first responders and the public to provide awareness of security concerns and preparedness.
- **Critical Infrastructure Protection**: Maintain and enhance programs to appropriately secure railroad critical infrastructure.

II. Programming Priorities

Table 6: Freight Rail Security Goals

NSTS Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience	
Activity 1	**Security Planning**: Railroads that transport Rail Security Sensitive Materials (RSSM) in High-Threat Urban Areas (HTUAs) have developed and implemented security plans
Activity 2	**Security Training**: Railroads that transport RSSM in HTUAs train frontline employees in security awareness on a triennial basis
Activity 3	**Security Exercises**: Railroads that transport RSSM in HTUAs conduct or participate in security exercises to improve security preparedness and resilience
Activity 4	**Risk Reduction**: Rail Transport of RSSM Materials: Rail carriers, shippers, and receivers of RSSM materials continue to apply measures that mitigate security risk
Activity 5	**Risk Reduction**: Promote utilization of risk-based and unpredictable security activities to mitigate terrorist risk to critical infrastructure and operations

NSTS Goal 2: Enhance effective domain awareness of transportation systems and threats	
Activity 1	**Intelligence and Security Information Sharing**: Ensure delivery of timely, meaningful, and actionable intelligence and security information products to rail security coordinators
Activity 2	**Community Outreach**: Railroads that transport RSSM in HTUAs engage in initiatives that provide awareness of security concerns and preparedness to local emergency response agencies and the public as appropriate

NSTS Goal 3: Safeguard privacy, civil liberties, and civil rights; and the movement of people and commerce	
Activity 1	Develop policy pursuant to applicable privacy, civil liberties, and civil rights laws and regulations

III. Challenges, Opportunities, and Path Forward

Table 7: Freight Rail Challenges, Opportunities, and Path Forward

Challenges or Opportunities	Path Forward
Physical and Cyber Security Operations and Practices: Securing critical infrastructure in an evolving threat environment	• Set priorities for action jointly, through government-industry consultations, and work in concert to meet them through enhanced coordination procedures and security-related capabilities • Establish metrics used to prioritize risk and manage investment in risk mitigating technologies and operations • Manage cybersecurity risks by improving system protections and resilience, facilitating security awareness, and promoting voluntary, collaborative, and sustainable community action as described in EO 13636 *Improving Critical Infrastructure Cybersecurity*
Stakeholder Relations and Information Sharing: Maintaining effective communications within the rail community to ensure sustained situational and security awareness and to define risk-based priorities and the means to attain them	• Improve effectiveness of collaborative exchanges between government and industry through joint consultations, exercises, training and awareness initiatives, and other appropriate venues • Pursue innovative approaches to enhance and expand information and intelligence sharing with key stakeholders • Apply industry reports of significant security concerns more effectively in analyses for patterns or trends, and in the formation of security policies and guidance

Highway and Motor Carrier Security Plan

I. Introduction

A. Overview

The Highway and Motor Carrier (HMC) Security Plan establishes risk-based priorities to protect the nation's roads, bridges, tunnels, cargo carriers, and travelers from attacks or use by terrorists. The strategic priorities expressed in the HMC Security Plan represent the collaborative view of the mode's owners, operators, and federal and SLTT governments. These organizations coordinate security initiatives and achieve strategic efficiency via alignment or consolidation of federal, state, and private programs. The HMC Security Plan recognizes some risks are persistent due to the dynamic nature of business ownership and uncertainty associated with the adversaries' intents and capabilities. The priorities described in this plan narrow security gaps that provide opportunities for terrorists. This plan meets the legislative requirements of the IRTPA of 2004 (as amended).[28]

1. Sector and Risk Profile

The highway system, commercial trucking, and passenger bus operations are an integral part of the Nation's economy and way of life. Free movement of raw and finished products along an unimpeded supply chain is essential for national and global markets. Critical highway transportation infrastructure provides the framework to move people and goods. Large-scale disruptions of these systems may adversely affect the Nation's economy and global markets.

More than a half billion passengers travel over the Nation's roads via school and over-the-road buses annually. Terrorists may attack highway infrastructure or buses directly or use vehicles carrying toxic or explosive cargoes as weapons to attack infrastructure.

2. Risk Scenarios[29]

The HMC attack scenarios influence the development of risk-based priority planning. These attack scenarios include:

- Attacks using IEDs or Vehicle-Borne IEDs on critical infrastructure such as bridges or tunnels;
- Small arms or IED attacks on passenger or school buses;
- A direct attack using a truck or vehicle loaded with explosives or toxic materials as a weapon against people or property; and
- Intentional contamination of food products during transportation.

[28] 49 U.S.C. §114(s)
[29] TSSRA 3.0 2014 and 2014 QHSR p. 47

B. Risk-Based Priorities

The risk-based priorities derived from the threat and attack scenarios described in the previous section provide the strategic focus for the activities to reduce terrorism risks. The priorities and activities in the following section will enhance security preparedness of the HMC mode overall and reduce risks associated with other types of incidents:

- Protect passengers on commercial, charter, and school buses;
- Protect critical bridges and tunnels;
- Protect shipments of HAZMAT and other security sensitive materials;
- Protect food shipments of higher concern from intentional contamination;
- Improve quality and timeliness of threat information and intelligence sharing;
- Improve personnel security credentialing and vetting programs;
- Enhance frontline employee security training and awareness; and
- Update critical asset assessments.

II. Programming Priorities

Table 8: Highway and Motor Carrier Security Goals

Goal 1: Manage risks of terrorist attacks and enhance resilience of highway and motor carrier transportation systems	
Activity 1	Identify, assess, and remediate vulnerabilities of our Nation's most critical highway infrastructure
Activity 2	Conduct Baseline Assessment for Security Enhancement assessments to assess and evaluate the security management and security programs of U.S. highway transportation providers
Activity 3	Establish exercise program to evaluate the resilience of over-the-road-bus operations to terrorist attack
Activity 4	Promote utilization of risk-based, unpredictable, and high visibility security activities to mitigate terrorist risk to critical infrastructure and operations

Goal 2: Enhance effective domain awareness of transportation systems and threats	
Activity 1	Improve the timeliness and quality of unclassified threat and security information shared with key stakeholders
Activity 2	Conduct periodic exercises of classified information dissemination to assure effectiveness
Activity 3	Enhance the use of Homeland Security Information Network (HSIN) through joint modal working groups
Activity 4	Collaboratively develop, maintain, revise, and disseminate industry security "Best Practices" to key stakeholders/stakeholder organizations

Goal 3: Safeguard privacy, civil liberties, civil rights, and the legitimate movement of people and commerce	
Activity 1	Promote modal supply chain security strategies using the Intermodal Security Training and Exercise Program (I-STEP) and the Exercise Information System
Activity 2	Apply privacy, civil liberties and civil rights laws, and regulations in policy development

III. Challenges, Opportunities, and Path Forward

Table 9: Highway and Motor Carrier Security Goals

Challenge or Opportunities	Path Forward
Information Sharing: Identifying and meeting stakeholder information sharing expectations and disseminating timely and actionable unclassified intelligence information to key modal partners	• Continue refining and improving classified information sharing processes • Develop a customer satisfaction "survey" for information product users • Maintain current contact data and manage communications channels across the mode
Training: Changing threats and personnel turnover require continual updating of security training	• Transition First Observer™ to a web-delivered training program • Continue to share relevant security information, guidance, and current training materials to stakeholders to enhance security training programs
Technology: Security measures, such as tracking security-sensitive shipments, are technology intensive and costly. Similarly, effective communications, particularly for emergencies, require reliable and compatible equipment to coordinate response among emergency and law enforcement officials	• Engage stakeholders to encourage resourcing solutions for maintaining compatible communications, Global Positioning Systems, and industrial control technologies • Transition First Observer™ to a web-delivered training program • Continue to develop guidance and training materials in electronic format to make accessibility to stakeholders more efficient

Mass Transit and Passenger Rail Security Plan

I. Introduction

A. Overview

The Mass Transit and Passenger Rail (MTPR) Security Plan establishes the national goals, objectives, and initiatives to protect the Nation's public transportation systems from terrorist attacks. The security priorities for the MTPR were established in collaboration with government and industry partners. The MTPR Security Plan addresses the requirements of the IRTPA of 2004 (as amended).[30]

1. Risk Profile

Attacks on transit services worldwide indicate these systems are potential targets for terrorists in the United States. MTPR systems are difficult to protect due to open infrastructure, high concentration of travelers, and multiple access areas with limited inspection and control points. Risks increase in urban areas due to the convergence of multiple transit systems and the higher densities of travelers at intermodal terminals. These systems typically have fixed, publicly accessible transit schedules. The open access to transit conveyances and the absence of passenger screening present inherent vulnerabilities to hostile actions by lone actors or tactical terrorist teams. Elevated risks are also associated with underground and underwater tunnels, common to many MTPR routes.

Passenger railroads operate on freight railroad routes across a significant portion of the Nation. Consequently risks to freight rail operations also present risks topassenger operations .

2. Risk Scenarios[31]

MTPR attack scenarios include:

- IED attacks on trains or infrastructure;
- Active-shooter situations;
- Sabotage of control systems; and,
- Chemical/biological attack.

[30] 49 U.S.C. §114(s)
[31] TSSRA 3.0 2014

B. Risk-based Priorities

- Secure nationally significant transit and rail infrastructure through the implementation of counterterrorism and risk reduction measures;
- Share threat information in a timely, accurate, and actionable manner;
- Improve operator and responder preparedness to prevent, mitigate, and respond to terrorist attacks;
- Promote best practices for security planning, assessments, training, and exercises; and
- Expand participation in the R&D process to identify technology solutions for security challenges.

II. Programming Priorities

Table 10: Mass Transit and Passenger Rail Security Goals

NSTS Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience	
Activity 1	Promote random, high-visibility security activities such as VIPR teams, mobile screening, electronic detection devices, and K9 detection teams at critical mass transit and passenger rail systems/infrastructure/facilities. Establish exercise program to test and improve MTPR resilience
Activity 2	Identify, assess, and remediate vulnerabilities for the Nation's most critical mass transit and passenger rail systems
Activity 3	Reduce risk of terrorist attacks in the Nation's highest-risk transit systems using Baseline Assessments for Security Enhancement

NSTS Goal 2: Enhance effective domain awareness of transportation systems and threats	
Activity 1	Evaluate and improve the quality of intelligence and information products and the unclassified information delivery system provided to the mass transit and passenger rail community
Activity 2	Promote use of effective public awareness campaigns in MTPR communities
Activity 3	Encourage private sector participation in the R&D process

NSTS Goal 3: Safeguard privacy, civil liberties, and civil rights; and the movement of people and commerce	
Activity 1	Apply privacy, civil liberties and civil rights laws, and regulations in policy development

III. Challenges, Opportunities, and Path Forward

Table 11: Mass Transit and Passenger Rail Challenges, Opportunities, and Path Forward

Challenges or Opportunities	Path Forward
Security Operations and Practices: Determining the transit industry baseline measures against the MTPR Strategy	• Evaluate data collection and validation options
Security Operations and Practices: Increasing operational deterrence at high-risk transit stations	• Continue to prioritize Transit Security Grant Program funding for public awareness campaigns, anti-terrorism law enforcement positions, and preparedness drills and exercises • Use the I-STEP program to enhance preparedness capabilities for transit systems
Security Operations and Practices: Securing the critical infrastructure on the Top Transit Asset List in an evolving threat environment	• Continue to engage with industry partners who have assets on the Top Transit Asset List to evaluate current remediation status and efforts • Prioritize Transit Security Grant Program funding to harden assets on the Top Transit Asset List
Security Operations and Practices: Assuring the security of cyber systems in public transportation for sensitive, networked systems such as operational controls, secure access, and signals	• Manage cybersecurity risks by improving system protections and resiliency, facilitating security awareness, and promoting voluntary, collaborative, and sustainable community action as described in Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*
Recovery and Resilience: Collaboratively developing actions and strategies that improve modal resilience	• Using the I-STEP program to engage the private sector through the mass transit and passenger rail SCC, SLTT, and federal governmental partners through the mass transit Government Coordinating Council to improve preparedness and resilience to a catastrophic incident

Pipeline Security Plan

I. Introduction

A. Overview

The Pipeline Security Plan establishes the strategic approach the pipeline community will take to secure the Nation's pipeline transportation systems from terrorist attacks and to enhance the systems' resilience despite disruptions. This Plan defines national pipeline security goals, objectives, and activities developed with government and industry stakeholders to reduce risks to nationally significant pipeline systems. This plan addresses the requirements of IRTPA of 2004 (as amended).[32]

1. Sector Profile

The national pipeline system consists of more than 2.5 million miles of networked pipelines transporting hazardous liquids, natural gas, and other liquids and gases for energy needs and manufacturing. Pipelines are also used to transport toxic chemicals such as anhydrous ammonia. Pipelines for the transport of non-hazardous liquids, such as water, are not addressed in the Plan. The bulk of pipeline infrastructure is buried. However, operational elements such as compressors, metering, regulating, and pumping stations; aerial crossings; and storage tanks are typically found above ground. Pipeline products are "pushed" through pipelines under pressure. The flows are monitored and moderated through automated industrial control systems or Supervisory Control and Data Acquisition systems that use remote sensors, signals, and preprogramed parameters to activate valves and pumps to maintain flows within tolerances.

The pipeline community includes government entities, industry organizations, owners, and operators. DHS, the Department of Energy, and DOT manage governance of counterterrorism security jointly at the federal level. TSA, acting as the agent of DHS for pipeline security, co-chairs the mode's Government Coordinating Council. Government receives industry advice through the Pipeline SCC. These councils are chartered elements of the Critical Infrastructure Partnership Advisory Committee.

2. Risk Profile

The national pipeline system and associated facilities are vulnerable to terrorist attacks because of their stationary nature, volatility of transported products, and the dispersed nature of pipeline networks spanning urban and outlying areas. A pipeline facility is especially vulnerable to an attack using an IED. Damage and disruption could also result from the use of standoff weapons. The dependence of pipelines on automated controls makes them susceptible to cyber attacks.

[32] 49 U.S.C. §114(s).

The consequences of these attacks may include supply chain disruption and hazardous material release. Pipeline disruptions may adversely impact the Nation's economy and in the most extreme cases may impact public health and national security. Minor disruptions may result in commodity price increases. Prolonged pipeline disruptions could lead to widespread energy shortages, production delays affecting the plastics and pharmaceutical industries, as well as other industries relying on commodities or chemicals dependent on pipeline delivery systems.

3. Risk Scenarios[33]

The likely terrorist attack scenario is the deployment of an IED or Vehicle-Borne IED at locations where pipeline infrastructure is exposed and the greatest impacts felt, such as a city gate for a highly populated urban area.

The pipeline system's dependence on remote sensors to regulate operations exposes the system to cyber attacks. The potential disruptions and ease of conducting cyber attacks with low levels of investment and skill create opportunities for cyber attackers and increased risk for the mode.

B. Risk-Based Priorities

- Enhance deterrence and mitigate vulnerabilities within the top 100 most critical pipeline systems;
- Enhance pipeline system preparedness and resilience through robust exercises and training; and
- Improve domain awareness and information sharing.

[33] TSSRA 3.0 2014

II. Programming Priorities

Table 12: Pipeline Security Goals

NSTS Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience	
Activity 1	Promote utilization of risk-based, unpredictable, highly visible security activities to mitigate terrorist risk to critical infrastructure and operations
Activity 2	Identify, assess, and remediate vulnerabilities for assets of our Nation's most critical natural gas and hazardous liquid pipeline systems
Activity 3	Encourage pipeline sector engagement in the physical and cyber security research and development process

NSTS Goal 2: Enhance effective domain awareness of transportation systems and threats	
Activity 1	Evaluate and improve the information delivery system and the quality of intelligence and information products provided to the natural gas and hazardous liquid pipeline community to ensure that timely, accurate, and actionable information reaches "need to know" industry contacts
Activity 2	Assess opportunities for enhanced information sharing processes with the natural gas and hazardous liquid pipeline community through industry developed activities such as Information Sharing & Analysis Centers

III. Challenges, Opportunities, and Path Forward

Table 13: Pipeline Challenges, Opportunities and Path Forward

Challenge or Opportunity	Path Forward
Physical and Cyber Security Operations and Practices: Securing critical infrastructure in an evolving threat environment	• Establish metrics that can be used to prioritize investment in risk mitigating technologies and operations • Promote the adoption of "best practice" security measures by the natural gas and hazardous liquid pipeline industry • Manage cybersecurity risks by improving protections and resilience, facilitating security awareness and best practices, and promoting voluntary, collaborative, and sustainable community action consistent with EO 13636 *Improving Critical Infrastructure Cybersecurity*
Stakeholder Relations and Information Sharing: Maintaining domain awareness and effective communication within the pipeline community due to turnover of employees, the evolving threat environment, and the open nature of pipeline systems	• Improve effectiveness of collaborative exchanges through training, exercises, roundtables, and use of the Oil & Natural Gas portal on HSIN • Develop and implement initiatives to enhance and expand information and intelligence sharing with key stakeholders
Recovery and Resiliency: Collaboratively developing a methodology to measure resilience and the actions and strategies that improve resilience	• Engage the private sector, SLTT entities, as well as federal governmental partners to measure, and where appropriate, improve preparedness and resilience to a catastrophic incident involving critical pipeline systems

Appendix D
2014 Intermodal Security Plan

Homeland Security

Transportation Security Administration

Intermodal Security Plan Introduction

The Intermodal Security Plan meets the requirement in legislation to address the security of intermodal transportation.[34] Intermodal transportation moves "individuals and property in an energy efficient way" and consists of "all forms of transportation, functioning in a unified, interconnected manner."[35] The Intermodal Security Plan describes the risk-based, strategic approach to protect intermodal transportation from terrorist attacks and their consequences.

The secure and free movement of individuals is a cornerstone of our way of life. Intermodal transportation extends opportunities to every segment of the population by providing economical, convenient, and secure travel networks for local and long distance travel. Intermodal passenger operations include a mix of ground, rail, aviation, and marine transportation. Those movements are typically discrete, involving separate mode-specific security processes. For example, when passengers move from a mass transit system to an airport, they typically leave one security process and enter another. The surface, aviation, and maritime security plans of the NSTS address the security of the infrastructure and operations providing intermodal passenger service. Consequently, the Intermodal Security Plan does not focus on the intermodal movement of passengers and addresses the protection of the intermodal movement of supplies and products in the context of supply chain, postal, and parcel security.

[34] 49 U.S.C. §114(s)(3)(H)
[35] Intermodal Surface Transportation Efficiency Act of 1991 (Public Law 102–240, 105 Stat. 2177)

Global Supply Chain Security Plan

I. Introduction

A. Overview

The United States and nations around the world depend on the efficient and secure transit of goods through the global supply chain system. This trade is essential to the U.S. economy and the Nation's prosperity. The National Strategy for Global Supply Chain Security (NSGSCS), issued by the President in January 2012, establishes the U.S. policy to strengthen the global supply chain in order to protect the welfare and interests of the American people and to secure the Nation's economic prosperity. The NSGSCS goals, objectives, and initiatives are the basis for managing the risks of terrorist use of or attack on the transportation elements of the global supply chain.

The transportation community helps implement the NSGSCS through various security activities, including government-led initiatives and industry practices. The Aviation, Maritime, Freight Rail, Highway Motor Carrier, Mass Transit and Passenger Rail, and Pipeline modes focus on mitigating risk. The modes' security activities are inextricably linked to the global supply chain security. As the modes mitigate risks, the interconnected network of the global supply chain benefits from risk mitigation as a whole. Specific individual strategies and activities that mitigate risk are discussed in each respective modal security plan.

1. Global Supply Chain Profile

The global supply chain is the worldwide network of conveyances, infrastructure, services, and technologies that moves goods between points of origin and consumers. It is vital for U.S. prosperity and security. The transportation elements of the global supply chain include: shippers (suppliers) and freight forwarders; air, land, or sea carriers; intermodal nodes such as transfer points and distribution centers; and aviation, maritime, highway, rail, and pipeline infrastructure. The global supply chain also includes a parallel network to exchange information in electronic or paper form about goods moving through the supply chain. The global supply chain security community includes a wide variety of international and domestic government entities, shipping and logistics industries, and supporting industries providing technology and information services. The transportation elements of the supply chain serve all commercial and service sectors creating security dependencies that impact transportation risk valuations.

Global supply chain security includes programs, procedures, and technologies to address the risks of terrorists using the supply chain in an attack. The global supply chain community is composed of foreign and domestic governments, international and domestic industry organizations and the composition of federal, SLTT, and industry entities engaging in the movement of commerce.

2. Risk Profile[36]

Two main terrorist-related risks are associated with the movement of cargo across transportation modes and the supply chain network. The transportation elements of the supply chain can be used to attack other critical infrastructure and people, or themslves be the target of an attack.

The primary risk associated with cargo transportation is the exploitation and use of the modes as a means to deliver an attack or to transport weapons of mass effect. Successful detonation of a WMD in a densely populated area, or use of a transportation asset itself as a weapon (such as in the 9/11 attacks), can result in catastrophic human, psychological, and economic consequences.[37]

The second risk is the cargo transportation supply chain as the target of a terrorist attack. U.S. transportation infrastructure is mature, efficient, and ubiquitous, which makes the sector resilient. There are, however, key inter-modal maritime, land, and air facilities — and major transportation gateway cities (e.g., Chicago, Kansas City, Memphis, St. Louis, Indianapolis, Houston, New Orleans, Miami) — that are critical pathways among transportation modes and supply chain links. Significant disruption in any one of these critical nodes could cause cascading consequences across the transportation system and the global supply chain that rely on the system, resulting in significant social and economic consequences that could be felt far from the original point of disruption.

Furthermore, certain materials in the supply chain serve critical functions—for example, pharmaceuticals, chemicals, or military materials—and have limited supply chain pathways that may be attractive targets due to a lack of redundant transportation networks. Even a small-scale attack on the transportation components of these critical pathways could significantly impact the movement of a critical product to the consumer (e.g., a hospital) with limited supply chain alternatives, or cascade to other critical infrastructure sectors.

The risks associated with cargo transportation are tied to threats external and internal to supply chain networks. Understanding the threats and interdependencies within supply chain networks — and the associated modal risks — is critical to developing a comprehensive approach to transportation security.

B. Risk-Based Priorities

Risk reduction priorities in the Transportation Systems Sector that support the mitigation of global supply chain risks include:

[36] TSSRA 3.0 2014

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

- Credentialing trusted actors in the global supply chain;
- Risk segmentation, screening, and validation of the contents and provenance of domestic and international cargo;
- Advance notification to destination countries of cargo contents;
- Ensuring the security and integrity of cargo while in transit via the use of escorts, locks, and tamper-proof seals; and
- Inspecting cargo at points-of-entry.

II. Programming Priorities

Global supply chain security is driven by the dynamic and complex nature of international logistics. The United States and its international security partners secure inbound cargo and improve global supply chain security through a layered security approach beginning overseas with advance reporting (e.g., 24-Hour Advance Manifest Rule) and cooperative arrangements with foreign customs organizations such as the Container Security Initiative (CSI). These programs allow security officials to make security-based admissibility decisions on the goods being transported prior to arrival at U.S. ports. This effort is enabled by the use of advanced, rules-based information technology through CBP's Automated Targeting System and the National Targeting Center to identify the relative risk of an inbound shipment. This also enhances identification of high-risk shipments coming from non-CSI ports that require inspection upon arrival to the U.S. In addition, the Customs-Trade Partnership Against Terrorism provides an awareness of the security measures that participating importers and carriers intend to implement, a cooperative mechanism for communicating best practices within the supply chain community, and serves as a platform to expedite shipments from known shippers. Combined, these programs allow the industry to separate high-risk from low-risk cargo and focus inspection efforts on higher-risk shipments prior to entry into the United States.

Domestically, the sector supports the security of the supply chain through risk mitigation activities discussed within each of the transportation modal security plans. This layered approach to supply chain security is advanced through efforts in the Aviation, Maritime, Freight Rail, Highway and Motor Carrier, Mass Transit and Passenger Rail, and Pipeline transportation modes. For example, commercial drivers who transport hazardous materials or work within a port environment are vetted to limit the opportunity for known terrorists to work within the industry. The freight rail industry hardens the most critical structures so that assets essential for the safe and efficient flow of commerce are protected.

The following section lists the global supply chain security goals, objectives based on the Transportation System Sector's risk-based priorities, and key initiatives that support these goals and objectives.

Table 14: Global Supply Chain Security Goals

Goal 1: Foster and enhance resilience of the global transportation supply chain system	
Objective 1: Reduce systemic risk to a supply chain disruption prior to a potential nationally-significant event by using layered risk management principles	
Activity 1	**Resilience STAR™**: Private-public partnership that seeks to enhance resilience across national critical infrastructure sectors by providing measurable, industry-approved performance targets, which owners and operators voluntarily can meet to receive a "STAR" certification (DHS, industry)
Activity 2	**International Ship and Port Facility Security Code**: Establishes a standard of security requiring vessels and port facilities to conduct security assessments, develop security plans, and provide security officers. The United States implemented and exceeded the ISPS Code through regulations implementing the Maritime Transportation Security Act (DHS/USCG)
Activity 3	**Regulatory Oversight and Compliance:** Inspections and assessments of airports, airlines, freight rail, and other regulated entities (DHS/TSA)
Objective 2: Improve capacities to effectively collect, protect, analyze, and share supply chain information among stakeholders, and strengthen and grow stakeholder partnerships and collaboration	
Activity 1	**International Trade Data System**: Intended to eliminate redundant reporting requirements and speed cargo processing by collecting commercial data from industry and distributing it electronically to the appropriate regulatory agency (DHS)
Activity 2	**Automated Manifest System**: A cargo release notification and inventory control system that facilitates quicker release and identification of low-risk shipments (DHS)
Activity 3	**Air Cargo Advance Screening**: A pilot program TSA conducts in conjunction with CBP, which provides a capability to quickly respond to emerging threats to international inbound cargo. Air Cargo Advance Screening verifies that messaging streams are effective across all modes that file air cargo reporting data and provides timely validation that industry and the system have the capability to share messaging and screening shipping data at the last point of departure and non-last points of departure (DHS/TSA/CBP)
Objective 3: Ensure orderly resumption of commerce following a large-scale disruption	
Activity 1	**National Response Framework**: Provides context for how the whole community works together and the response efforts relate to other parts of national preparedness (DHS/USCG, SLTT, industry)
Activity 2	**National Incident Management System**: A standardized approach to incident management established in March 2004, intended to facilitate coordination between all responders (including all levels of government with public, private, and nongovernmental organizations) (DHS/USCG, SLTT, industry)
Activity 3	**Security Planning**: Recovery processes are a critical component of resilience and are included in the planning of most entities involved in the supply chain (DHS/USCG, SLTT, industry)

Goal 2: Enhance the efficient and secure movement of goods	
Objective 1: Mitigate and manage risks as early as possible in the global supply chain networks to promote the efficient flow of commerce	
Activity 1	**Transportation Worker Identification Credential (TWIC)**: A tamper-resistant biometric credential issued, after successful completion of a background check, to maritime workers requiring unescorted access to secure areas in ports and MTSA-regulated facilities; and readers connected to a central data bank of holders to confirm identity. (DHS/TSA/USCG)
Activity 2	**Hazardous Materials Endorsement Threat Assessment**: Requires a security threat assessment for any driver seeking to obtain, renew, or transfer a Hazardous Materials Endorsement on a state-issued commercial driver's license (DHS/TSA, DOT)
Activity 3	**Container Security Initiative (CSI)**: Supports CBP, working with host government Customs Services, to examine high-risk maritime containerized cargo at foreign seaports before it is loaded on board vessels destined for the United States (DHS/CBP)
Activity 4	**Automated Targeting System**: Performs transactional risk assessments and evaluates potential security risks posed by cargo arriving by sea, air, truck, or rail (DHS/CBP)
Activity 5	**International Port Security Program**: Assesses the effectiveness of anti-terrorism measures in foreign ports, conducts capacity building where gaps exist, and imposes conditions of entry on vessels arriving to the United States from ports with substandard security (DHS/USCG)
Objective 2: Enhance implementation of global supply chain-related standards, best practices, and guidelines and regulations allowing stakeholders to realize efficiencies while maintaining acceptable levels of security	
Activity 1	**Customs-Trade Partnership Against Terrorism (C-TPAT)** : A voluntary CBP-led supply chain security program focused on improving the security of private companies' supply chains with respect to terrorism (DHS/CBP)
Activity 2	**24-Hour Advanced Manifest Rule**: Rule requires carriers to submit a cargo declaration to CBP 24 hours before cargo is loaded onto vessels destined to the United States (DHS/CBP)
Activity 3	**Air Cargo Security Programs**: Collaborate with international associations and governments to harmonize supply chain regulations and standards such as the Joint Working Group On Advanced Cargo Information (DHS/TSA/CBP)
Objective 3: Improve situational awareness of terrorist threats to the global supply chain	
Activity 1	**Automated Commercial Environment**: The primary system for the trade community to report imports and exports and for the government to determine admissibility (DHS/CBP)
Activity 2	**HSIN and its Critical Infrastructure**: A secure network with a common set of information-sharing functions and tools for various private sector communities with common security interests (DHS, industry)
Activity 3	Work with the Directorate of National Intelligence, the Department of Defense, and Industry to develop cyber risk assessment capabilities that can address global supply chain security.

Objective 4: Improve industry involvement in the global supply chain Research and Development (R&D) process to improve security of goods in transit and minimize delays	
Activity 1	**Cargo and Supply Chain R&D Plan**: Developed to align technology needs with investments, including planning for future security hardware and systems upgrading (DHS/S&T/DNDO/USCG, industry)
Objective 5: Enhance the security of critical infrastructure and conveyances in order to protect the supply chain and nodes against terrorist attacks	
Activity 1	**Non-Intrusive Inspection Technology**: Allows the Federal Government to screen a larger portion of the stream of commercial traffic in less time while facilitating commerce (DHS/S&T/DNDO/USCG/CBP, industry)
Activity 2	**Air Cargo Security Programs**: Requires shippers, air forwarders, independent facilities and airlines to screen cargo before it is loaded aboard aircraft (DHS, FAA)
Activity 3	**96-Hour Advance Notice of Arrival**: Requires a vessel to notify the USCG 96 hours before arriving in a U.S. port to provide detailed information on the crew, passengers, cargo, and voyage history (DHS/USCG)
Activity 4	**High Interest Vessel Boarding**: All vessels are screened for security risk, and higher-risk vessels are targeted for boarding to ensure potential security issues (DHS/USCG)

III. Challenges, Opportunities, and Path Forward

Table 15: Global Supply Chain Challenges, Opportunities, and Path Forward

Challenge or Opportunities	Path Forward
The numerous entities involved in the supply chain make efficient information sharing difficult	• Develop innovative intelligence systems that will fuse and analyze information into reliable, actionable knowledge that can be easily used by decision-makers
Screening of inbound cargo	• Develop more efficient, non-intrusive cargo inspection technologies
Understanding the threats to and the vunerabilities of intermodal linkages and transition points	• Continue to work with the shipping community on industry best practices to mitigate risk at supply chain nodes and connecting pathways between • Leverage exercise capabilities such as I-STEP to test the security of the transportation elements of the supply chain
Improve coordination of the government's responsbilities for the interdepent functions of the global supply chain	• Continue updating the NSGSCS implementation process

Postal and Shipping Security Plan

I. Introduction

A. Overview

1. Purpose

The Postal and Shipping (P&S) Security Plan is intended to reduce the risks of terrorists using or attacking the P&S system, while enhancing system resilience, preserving commerce, and safeguarding privacy, civil rights, and civil liberties. The P&S Security Plan addresses a key part of the intermodal transportation security needs required by IRTPA of 2004 (as amended).[38]

2. Postal and Shipping Profile

As a part of the Nation's network of transportation systems, the P&S subsector receives, processes, transports, and distributes billions of letters and parcels annually. Every sector of the economy depends on P&S services to deliver products, supplies, parts, or correspondence. Further, businesses, government, and individuals rely on the continuity and timely functioning of P&S services to conduct vital business, medical, and personal transactions. P&S services are highly dependent on the Information Technology, Communications, Energy, and Transportation Systems Sectors.

Delivery of goods directly to consumers distinguishes P&S operations from the related supply chain operations for retailers and wholesalers. P&S-related deliveries serve the rapidly growing electronic shopping and mail order markets. U.S. e-commerce sales alone increased from $170 billion to more than $229 billion between 2010 and 2012—a 35 percent increase.[39] Projections suggest the trend will continue. For the P&S subsector, expanding e-commerce and mail order sales means growth in demand, capacity, and workforce and a challenge sustaining security.

The subsector risk is managed by government and industry partners. The industry is dominated by four large carriers – the United States Postal Service, United Parcel Service, Federal Express, and DHL International – that provide point-to-point delivery service. These integrated carriers and their supply chain partners own the vast majority of the sector's assets, systems, and networks. The other components of the subsector consist of smaller firms that provide international, national, regional, and local delivery and courier services, including carriers; mail preparers; mail management firms; state, local, tribal, military, and various other types of government-run or administered mail centers; priority medical transporters; and other specialized

[38] 49 U.S.C. §114(s)

[39] http://www.census.gov/econ/estats/2012/all2012tables.html (See historic table "U.S. Retail Trade Sales – Total and E-Commerce 2012 – 1998")

delivery services. Although much of the subsector is privately owned, there is a major government presence in the subsector through the U.S. Postal Service, DoD, and other government-owned and -operated mail centers and mail production facilities.

3. Risk Profile

A major disruption of P&S services could have a negative impact on business revenues, government operations, and the economy.

The P&S community includes numerous customer service locations and delivers mail and packages nationwide to individuals, businesses, and government offices. The subsector is vulnerable to being exploited by terrorists to receive materials or weapons or to deliver weapons to specific targets. Packages or mail could be used to deliver: chemical, biological, radiological, nuclear, or explosive devices.

Vulnerabilities are also associated with the large workforce and employee turnover rates. Due to the extensive openness of the P&S system, its numerous access points, and extensive delivery network, P&S frontline employee awareness and security threat assessments are key aspects of risk management. Security threats to the subsector also include physical intrusion into restricted facilities and insiders who may facilitate or participate in terrorist activities. Cyber systems are used extensively to track packages from origin to destination. The tracking systems are vulnerable to the manipulation of shipment data and circumvention of security controls.

B. Risk-Based Priorities

The P&S Subsector will address these risks by:

- Expanding risk assessments of high-volume mail distribution centers;
- Improving security of sensitive areas of P&S facilities;
- Increasing interaction with the Intelligence Community to facilitate threat awareness;
- Improving effectiveness of partnerships within the P&S Subsector and with other sectors;
- Enhancing frontline P&S employee security training; and
- Enhancing the vetting and credentialing of frontline employees.

II. Programming Priorities

The guiding principles for the P&S Subsector are to ensure resilience, ease of use, and public confidence by using a multilayered risk management approach that integrates public and private stakeholders. The subsector applies security measures to deny terrorists the ability to exploit the P&S system. Enhancement of the sector's partnerships and collaboration among Federal, SLTT, and private sector communities, both domestic and international, will improve the safety and security of the sector's assets.

The following section lists the goals and objectives for the P&S Subsector, and key initiatives that support them.

Table 16: P&S Security Goals

Goal 1: Manage risks to the P&S Subsector and enhance system resilience	
Objective 1: Improve deterrence and response to a national or regional terrorist emergency affecting the P&S Subsector	
Activity 1	Improve risk assessment processes (DHS/TSA, industry)
Objective 2: Minimize the risk of unauthorized individuals gaining access into secured areas	
Activity 1	Expand voluntary use of best-practice security protocols (DHS/TSA, industry)

Goal 2: Enhance effective domain awareness of P&S Subsector systems and threats	
Objective 1: Improve awareness of cross sector interdependencies	
Activity 1	Partner with industry and the Intelligence Community to facilitate threat awareness. Utilize the HSIN to communicate with the P&S community to retrieve and update information and intelligence. Work to develop a communications procedure for routine and incident-specific information sharing (DHS/TSA, industry)
Activity 2	Assess interdependencies of other sectors relying on P&S (DHS/TSA)

Goal 3: Safeguard privacy, civil liberties and civil rights, and the freedom of movement of people and commerce	
Objective 1: Minimize the security risks and delays in freight movement and reduce potential for adverse privacy, civil rights, and civil liberty impacts of security policies	
Activity 1	Enhance continuity of operational plans to ensure the sector can continue to move parcels and letters to intended recipients (DHS/TSA, industry)

III. Challenges, Opportunities, and Path Forward

Table 17: P&S Challenges, Opportunities, and Path Forward

Challenge or Opportunities	Path Forward
The evolving landscape for terrorist activity (methods and technology) is an ongoing challenge for the P&S Subsector Diverse protocols for international mail security create challenges for security managers globally	• Monitor and assess current security trends in the P&S community • Introduce or implement new concepts and technologies to combat threats • Initiate plans to harmonize regulations and standards for the application of air mail security controls