



# Transportation Systems Sector-Specific Plan

2015



Homeland  
Security



United States  
Department of Transportation

# Table of Contents

<b>Preface</b> .....	<b>ii</b>
<b>1. Executive Summary</b> .....	<b>1</b>
<b>2. Introduction</b> .....	<b>3</b>
2.1 Sector Vision and Mission .....	4
<b>3. Sector Overview</b> .....	<b>5</b>
3.1 Sector Risks .....	6
3.2 Sector Partners and Stakeholders .....	7
3.3 Cross-Sector Issues.....	10
<b>4. Sector Goals and Priorities</b> .....	<b>13</b>
<b>5. Achieving Sector Goals</b> .....	<b>14</b>
5.1 Risk Management .....	14
5.2 Critical Infrastructure and National Preparedness .....	17
<b>6. Measuring Effectiveness</b> .....	<b>19</b>
<b>Appendix A: Acronym List</b> .....	<b>23</b>
<b>Appendix B: Alignment with the NIPP 2013</b> .....	<b>25</b>
<b>Appendix C: Authorities</b> .....	<b>30</b>
<b>Appendix D: Glossary of Terms</b> .....	<b>31</b>

# Preface

As co-Sector-Specific Agencies (SSAs) for the Transportation Systems Sector (hereafter referred to as the Sector), the U.S. Department of Homeland Security (DHS)—with the Transportation Security Administration and the United States Coast Guard as executive agents for DHS—and the U.S. Department of Transportation are pleased to present the 2015 Transportation Systems Sector-Specific Plan (TS SSP). The TS SSP tailors the strategic guidance in the National Infrastructure Protection Plan 2013, *Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), to the unique operating and risk environment of the Sector.

The TS SSP is a planning tool for the SSAs, critical infrastructure owners and operators, and partners at the regional, State, local, tribal, and territorial levels. The TS SSP guides and integrates efforts to secure and strengthen the resilience of critical infrastructure, identifies the Sector’s security and resilience priorities, and describes the approach to managing critical infrastructure risk. It builds upon the 2010 TS SSP and aligns with other national strategies and plans that address preparedness to prevent, protect against, mitigate, respond to, and recover from manmade and natural hazards. The TS SSP is intended to focus the resources and programming of agencies and companies on collaboratively determined priorities for effective management of sector risks. It is not intended to replace agency- or company-specific planning documents or risk management processes.

The Sector’s security and resilience partners developed the TS SSP collaboratively to inform leaders in government and industry of recommended actions to implement the security and resilience goals of the NIPP 2013. The signatories encourage the Sector’s partners—who share responsibility for the security and resilience of transportation systems and assets—to adopt or contribute to the recommended priorities and activities and to participate in follow-up efforts to determine the effectiveness of activities recommended in this Plan. The Sector will periodically review and update the TS SSP and its measures of effectiveness.



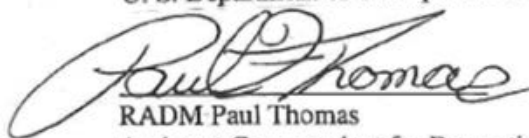
Ms. Caitlin Durkovich  
Assistant Secretary  
Office of Infrastructure Protection  
U. S. Department of Homeland Security



Mr. Michael W. Lowder  
Director  
Office of Intelligence, Security and  
Emergency Response (S-60)  
U. S. Department of Transportation



Mr. Eddie D. Mayenschein  
Assistant Administrator  
Office of Security Policy and Industry  
Engagement  
Transportation Security Administration



RADM Paul Thomas  
Assistant Commandant for Prevention Policy  
U. S. Coast Guard

# 1. Executive Summary

The purpose of the 2015 Transportation Systems Sector-Specific Plan (TS SSP) is to guide and integrate efforts to secure and strengthen the resilience of transportation infrastructure and to describe how the Transportation Systems Sector (hereafter referred to as the Sector) contributes to the overall security and resilience of the Nation's critical infrastructure, as set forth in Presidential Policy Directive 21 (PPD-21), *Critical Infrastructure Security and Resilience*. The TS SSP tailors the strategic guidance provided in the National Infrastructure Protection Plan 2013, *Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013), to the unique operating conditions and risk landscape of the Nation's varied transportation systems.

The TS SSP represents a collaborative effort among Federal departments and agencies; State, local, tribal, and territorial (SLTT) governments; non-governmental organizations; and public and private critical infrastructure owners and operators to achieve shared goals and priorities to reduce critical infrastructure risks. It also reflects the maturation of the Sector partnership and the progress made by the Sector since the 2010 TS SSP to address evolving risks as well as operating and policy environments.

This Plan describes an approach to manage security and resilience efforts while enhancing the efficient use of the capabilities and resources of the Sector's government and industry partners. Transportation systems encompass diverse and interconnected networks of fixed and mobile assets that provide essential services for the Nation's livelihood and economic prosperity.

The Sector's mission is to continuously improve the security and resilience posture of the Nation's transportation systems in order to ensure the safety and security of travelers and goods. Its vision is a secure and resilient transportation system, enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties.

Transportation systems provide lifeline services for communities and are vitally important for response and recovery operations. The vast network of public and private critical infrastructure owners and operators, the infrastructure and services they manage, and the extensive interdependencies among the transportation modes and other sectors indicate the need for coordinated planning and investments to manage all hazards efficiently and effectively. Government entities and transportation critical infrastructure owners and operators share responsibility for managing the security and resilience of the Sector's infrastructure and systems.

The identification of critical transportation infrastructure requires consideration of Federal, State, regional, and local jurisdictional interests and a variety of hazards. At the national level, critical infrastructure in each of the Sector's four subsectors—aviation, maritime, surface, and postal and shipping—contribute to national security, economic stability, and public health and safety. At the regional, State, and local levels, the criticality of infrastructure is primarily determined by the business, lifestyle, and emergency needs of the community.

To secure transportation systems from risks such as natural disasters and manmade threats, security managers conduct assessments of physical, human, and cyber elements of critical infrastructure. Cyber-related risks are an increasing concern as transportation operations become more reliant on those technologies. Transportation is also sensitive to risks in interdependent sectors: Chemical,

Communications, Critical Manufacturing, Dams, Defense Industrial Base, Emergency Services, Energy, Food and Agriculture, Information Technology, and Water and Wastewater Systems. In addition, the Nation's reliance on foreign markets, international mobility, and global supply chains requires the consideration of risks to critical international transportation infrastructure. Multiple Federal departments and private enterprises, in coordination with the Department of State, contribute to the development of security protocols through international agreements and regulatory bodies, such as the International Maritime Organization, the World Customs Organization, the International Civil Aviation Organization, and the Universal Postal Union.

The Department of Homeland Security (DHS) and the Department of Transportation (DOT)—co-Sector-Specific Agencies (co-SSAs) identified in PPD-21—jointly prepared the TS SSP in collaboration with the Sector's partners. The Plan defines the roles and responsibilities of government and private industry, and it proposes goals, priorities, and activities to manage risks and to contribute to national security and resilience goals in NIPP 2013.

The TS SSP identifies the following goals:

- Goal 1: Manage the security risks to the physical, human, and cyber elements of critical transportation infrastructure.
- Goal 2: Employ the Sector's response, recovery, and coordination capabilities to support whole community resilience.
- Goal 3: Implement processes for effective collaboration to share mission-essential information across sectors, jurisdictions, and disciplines, as well as between public and private stakeholders.
- Goal 4: Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard U.S. national interests.

The Sector applies the NIPP Risk Management Framework (RMF) to understand and manage security and resilience risks, and the Sector employs a variety of assessment tools, exercises, analyses, and plans to set risk-based security and resilience priorities and to identify activities to achieve those priorities. The TS SSP identifies 24 activities that include specific actions and processes to address the NIPP 2013 Calls to Action and the Joint National Priorities (JNPs). The selected activities also consider Presidential Policy Directive 8 (PPD-8), *National Preparedness*, and the development of core capabilities for the protection, prevention, mitigation, response, and recovery missions of the National Preparedness System (NPS).

The TS SSP identifies activities that include conceptual approaches—qualitative and quantitative—to measure their effectiveness. Officials responsible for implementing the activities should initiate the approach to measure its effectiveness.

## 2. Introduction

PPD-21 names 16 critical infrastructure sectors and the executive departments responsible for overseeing security and resilience in each sector. The directive designates DHS and DOT as co-SSAs for the Transportation Systems Sector. DHS delegates its co-SSA responsibilities to the Transportation Security Administration (TSA) and the United States Coast Guard (USCG). DOT, TSA, and the USCG jointly perform the co-SSA functions through a steering group and co-leadership of Government Coordinating Councils (GCCs). Close coordination among the co-SSA partners ensures unified Federal representation for security partners.

PPD-21 recognizes the importance of effective partnerships with critical infrastructure owners and operators and SLTT entities and requires DHS to update the NIPP. NIPP 2013, *Partnering for Critical Infrastructure Security and Resilience*, provides a model to facilitate public-private partnerships. GCCs receive advice on the development of voluntary security and resilience initiatives from private sector critical infrastructure owners and operators through Sector Coordinating Councils (SCCs). There are seven such partnerships serving the key communities in the Sector identified in section 3. The councils enhance the mutual awareness and understanding of security and resilience issues, share intelligence and risk information, and develop recommended practices. The security partners determine risk-based priorities and develop joint plans for the effective and efficient use of resources as well as the coordination of shared responsibilities.

The Sector's security partners—including Federal departments and agencies, SLTT governments, nongovernmental organizations, and public and private critical infrastructure owners and operators—collaborated to prepare the TS SSP, which describes shared goals, priorities, and activities to mitigate critical infrastructure risks. The Plan builds on the progress made in the Sector since the 2010 TS SSP and addresses evolving risk, operating, and policy environments. The TS SSP also considers the core capability needs of the five NPS mission areas: prevention, protection, mitigation, response, and recovery.

The TS SSP updates the Sector's cybersecurity efforts to align with growing concerns about cyber threats and their consequences. The Plan advances implementation of the President's Cybersecurity initiatives in Executive Order (EO) 13636, *Enhancing Critical Infrastructure Cybersecurity*.

The TS SSP also incorporates elements of the 2014 National Strategy for Transportation Security. The Strategy is the governing document for the Sector's Federal counterterrorism efforts, developed in consultation with transportation industry, government, and labor representatives to manage security risks to transportation assets that, "in the interests of national security and commerce, must be protected from attack or disruption by terrorist or other hostile forces." The Strategy is the primary source for security-related programming in the TS SSP, which includes programming for security and resilience for all hazards—manmade and natural.

The 2015 TS SSP does not create, alter, or impede the ability of Federal departments and agencies to perform their responsibilities under law. This plan does not create any right or benefit, substantive or procedural, enforceable by law or in equity against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.

## 2.1 Sector Vision and Mission

The Sector supports the physical, cybersecurity, and resilience objectives of PPD-21 and the NIPP 2013. The Sector's mission identifies the unifying purpose of its public and private security partners. Sustained accomplishment of the mission will enable the Sector to realize its vision.

### **SECTOR VISION**

A secure and resilient transportation system, enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties

### **SECTOR MISSION**

Continuously improve the security and resilience posture of the Nation's transportation systems in order to ensure the safety and security of travelers and goods

# 3. Sector Overview






## Transportation Sector Profile

### Assets and Impacts

#### Owners & Operators

- Public and private companies own and operate the Sector's critical infrastructure, and they have primary responsibility for the security and resilience of their operations.
- Owners and operators conduct risk assessments, develop plans, implement risk management programs, and conduct training and exercises.
- Owners and operators voluntarily participate with government to establish priorities and coordinate activities to achieve optimal effectiveness and efficiency.

<p><b>Aviation</b></p> <ul style="list-style-type: none"> <li>➢ Composed of airports, heliports, seaplanes bases, support services, air traffic control, and navigation facilities.</li> <li>➢ Approx. 19,700 airports in the U.S., with 500 offering commercial service.</li> <li>➢ Approx. 780,000 passenger flights take place across the U.S. monthly.</li> </ul> 	<p><b>Maritime</b></p> <ul style="list-style-type: none"> <li>➢ Geographically complex and diverse system consisting of waterways, ports, and intermodal landslide connections.</li> <li>➢ Consists of nearly 95,000 miles of coastline, 361 ports, more than 25,000 miles of navigable waterways, and more than 29,000 miles of Marine highway.</li> </ul> 
--	---

<p><b>Freight Rail</b></p> <ul style="list-style-type: none"> <li>➢ Approx. 1.33 million freight cars in service. (2013)</li> <li>➢ Consists of 140,000 miles of active rail track.</li> <li>➢ Transports more than 70% of all U.S. coal shipments.</li> <li>➢ Approx. 73 billion in operating revenue for the 7 Class 1 railroads. (2013)</li> </ul> 	<p><b>Highway &amp; Motor Carrier</b></p> <ul style="list-style-type: none"> <li>➢ Composed of bridges, major tunnels, trucks carrying hazardous materials, other commercial freight vehicles, motor coaches, school buses, and key intermodal facilities.</li> <li>➢ Includes nearly 4 million miles of roadway, more than 600,000 bridges, and 400 tunnels.</li> </ul> 	<p><b>Pipeline</b></p> <ul style="list-style-type: none"> <li>➢ More than 2.5 million miles of pipelines span the U.S. to transport nearly all of the natural gas and approx. 65% of hazardous liquids, including crude and refined petroleum.</li> <li>➢ Above-ground assets include compressor stations and pumping stations.</li> </ul> 	<p><b>Postal &amp; Shipping</b></p> <ul style="list-style-type: none"> <li>➢ Includes large integrated carriers, regional and local courier service providers, mail services and mail management firms, and chartered and delivery services.</li> <li>➢ Approx. 720 million letters and packages moved each day.</li> </ul> 	<p><b>Mass Transit</b></p> <ul style="list-style-type: none"> <li>➢ Includes transit buses, trolleybuses, monorails, heavy rail (subway), light rail, passenger rail, commuter rail, and vanpool/rideshare.</li> <li>➢ 10.3 billion passenger trips in 2012.</li> </ul> 
---	--	--	--	---

<p><b>9.3% of 2013 U.S. GDP*</b> was supported by the Transportation Sector</p>	<p><b>Approx. 6% of the 2013 U.S. Employed Population**</b> worked in the Transportation Sector</p>	<p><b>Approx. 19.6 Billions of Tons of Goods***</b> were shipped in 2014</p>
---	---	--

### Cross-Sector Dependencies

The Transportation Systems Sector touches everyone in some way. Personal mobility, the movement of raw materials to factories, the delivery of refined or manufactured products to buyers, and the shipment of agriculture and food products are just a few of the ways the Nation depends on transportation for its livelihood and economic stability. The Transportation Systems Sector has many interdependencies with other critical infrastructure sectors, as all sectors rely on transportation services to some extent for normal operations and to a greater extent for emergency response and recovery. The Sector's central role in supply chain operations creates other dependencies that impact businesses, communities, and individuals



\*[http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national\\_transportation\\_statistics/html/table\\_03\\_09.html](http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_03_09.html). Accessed August 13, 2015.  
 \*\*TSA OSPIE Cross Modal Division Analysis of Bureau of Transportation Statistics and Bureau of Labor Statistics  
[http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national\\_transportation\\_statistics/html/table\\_03\\_24.html](http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/publications/national_transportation_statistics/html/table_03_24.html). Accessed August 13, 2015.  
<http://data.bls.gov/pdq/SurveyOutputServlet>. Accessed August 13, 2015.  
 \*\*\*[http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/TITUS\\_2013.pdf](http://www.rita.dot.gov/bts/sites/rita.dot.gov.bts/files/TITUS_2013.pdf). Accessed August 13, 2015.



## **3.1 Sector Risks**

Risks to critical transportation infrastructure include natural disasters as well as manmade physical and cyber threats. Manmade threats include terrorism, vandalism, theft, technological failures, and accidents. Cyber threats to the Sector are of concern because of the growing reliance on cyber-based control, navigation, tracking, positioning, and communications systems, as well as the ease with which malicious actors can exploit cyber systems serving transportation.

### **3.1.1 Terrorism**

Terrorist attacks, whether physical or cyber, can significantly disrupt vital transportation services and cause long-term sociological and economic consequences. The risk of a terrorist attack on transportation infrastructure is typically assessed using attack scenarios to evaluate the threats, vulnerabilities, and consequences. DHS agencies use a variety of methods for assessing risks. The Transportation Sector Security Risk Assessment (TSSRA) is an annually-updated, scenario-driven evaluation of risks that compares the aviation, mass transit, freight rail, highway and motor carrier, and pipeline modes. For example, the TSSRA 4.0 concludes that the aviation mode has the highest risk of a terrorist attack compared to other modes. TSSRA does not include nuclear threat scenarios because the Radiological and Nuclear Terrorism Risk Assessment, led by the DHS Domestic Nuclear Detection Office, specifically focuses on radiological and nuclear risk.

The USCG uses the Maritime Security Risk Analysis Model (MSRAM) as a terrorism risk management tool. At the national level, MSRAM supports the USCG's strategic planning efforts. MSRAM also informs a variety of port and waterway security risk decisions, and its results respond to the decision makers' needs as data and situational assumptions change.

### **3.1.2 Aging Infrastructure**

The condition of the Nation's transportation infrastructure is a particular concern because of the advanced age and deterioration of many structures throughout the Nation's transportation network. Aging infrastructure threatens the resilience of these systems and can multiply risks from other factors (such as manmade or natural disasters). The effects of a natural disaster, for example, can be much worse when combined with aging infrastructure. The impact of a loss of a key node or asset, such as a bridge, poses an immediate threat to users and can have cascading impacts to passenger and freight movement, as well as potentially large-scale impacts (such as supply chain disruption).<sup>1</sup>

### **3.1.3 Natural Disasters, Global Climate Change, and Extreme Weather Events**

Natural disaster risks to transportation systems include earthquakes, wildfires, flooding, and extreme weather events, such as blizzards, hurricanes, tornados, and droughts, all of which have the potential for widespread disruption of transportation services. Risks from natural disasters have a varying regional or local relevance because of prevailing weather patterns, geological trends, topographical features, and population density.

---

<sup>1</sup> "A Bridge Too Far: Repairing America's Aging Infrastructure" *Risk Management Magazine*, February 2014.

Studies such as the U.S. National Climate Assessment link certain extreme weather events with climate change. These events have become more frequent and have exacerbated existing vulnerabilities in our Nation's aging transportation infrastructure.<sup>2</sup> The Third National Climate Assessment (released in 2014) found that a rise in sea level, heavy downpours, and extreme heat are damaging infrastructure, and that vulnerabilities to damage are projected to increase with continued climate change.<sup>3</sup>

Findings for the Sector include:

- A rise in sea level, coupled with storm surges, will continue to increase risk of major coastal impacts on transportation infrastructure, including temporary and permanent flooding of airports, ports and harbors, roads, rail lines, tunnels, and bridges;
- Extreme weather events currently disrupt transportation networks in all areas of the country, and projections indicate that such disruptions will increase; and
- Climate change impacts will increase total costs to the Nation's transportation systems and its users, but these impacts can be reduced through a variety of adaptive actions.

## 3.2 Sector Partners and Stakeholders

Sector partners include individuals, groups, and organizations that have responsibility for the security and resilience of the Sector's assets, systems, and networks. Federal, SLTT, and foreign governmental entities; critical infrastructure owners and operators; and regional organizations and coalitions are responsible for critical infrastructure security and resilience. Academic and professional entities, international organizations, nonprofit employee representative organizations, volunteer organizations, and the public are important community stakeholders. The Sector engages its partners through a collaborative process to determine Sector goals, priorities, and risk methodologies as they relate to the physical, human, and cyber elements of critical transportation infrastructure.

### 3.2.1 Sector-Specific Agencies

SSA responsibilities, as stated in NIPP 2013, include engaging partners in cooperative processes to:

- Coordinate with DHS and other Federal departments and agencies;
- Collaborate with critical infrastructure owners and operators, independent regulatory agencies, and SLTT entities;
- Serve as a day-to-day Federal interface for the dynamic prioritization and coordination of Sector activities;
- Carry out incident management responsibilities consistent with statutory authority and other appropriate policies, directives, or regulations;

---

<sup>2</sup> "Overview of Climate Change Impacts in the United States: The Third National Climate Assessment." U.S. Global Change Research Program, 2014. Web. <<http://www.globalchange.gov/browse/reports/overview-climate-change-impacts-united-states-third-national-climate-assessment>>. Accessed August 13, 2015.

<sup>3</sup> "Highlights from 2014 National Climate Assessment." *GlobalChange.gov*. U.S. Global Change Research Program, 2014. Web. <<http://nca2014.globalchange.gov/highlights>>. Accessed August 13, 2015.

- Provide, support, or facilitate technical assistance and consultations for that sector to identify vulnerabilities and help mitigate incidents, as appropriate; and
- Support the Secretary of Homeland Security's statutorily required reporting requirements by providing, on an annual basis, sector-specific critical infrastructure information.

**Department of Homeland Security.** The DHS National Protection and Programs Directorate (NPPD) administers various roles and responsibilities in PPD-21. In addition, U.S. Customs and Border Protection (CBP) and the Federal Emergency Management Agency (FEMA) contribute significantly to the transportation security and resilience mission. As the delegated leads for DHS co-SSA responsibilities, TSA and USCG have unique responsibilities described below.

- **Transportation Security Administration.** The Aviation Transportation Security Act assigns TSA the Federal responsibility for security in all modes of transportation. TSA addresses responsibilities for maritime security by supporting the USCG in exercising its broad statutory authorities and responsibilities for maritime safety, security, and resilience. In addition, TSA consults or collaborates, as directed in various statutes, with DOT in performing these duties.
- **United States Coast Guard.** The USCG has the primary responsibility for the safety, security, and environmental protection of the maritime domain, including enforcing customs and immigration laws at sea, managing the responses to incidents impacting the Federal navigable waters and ports, and coordinating and expediting the recovery of maritime transportation system. The USCG engages these responsibilities through a network of 43 Area Maritime Security Committees (AMSCs) in each Captain of the Port zone. The AMSC's are the cornerstones of security in the Nation's ports. In addition, the USCG benefits from the contributions of several advisory committees and other industry engagement forums.

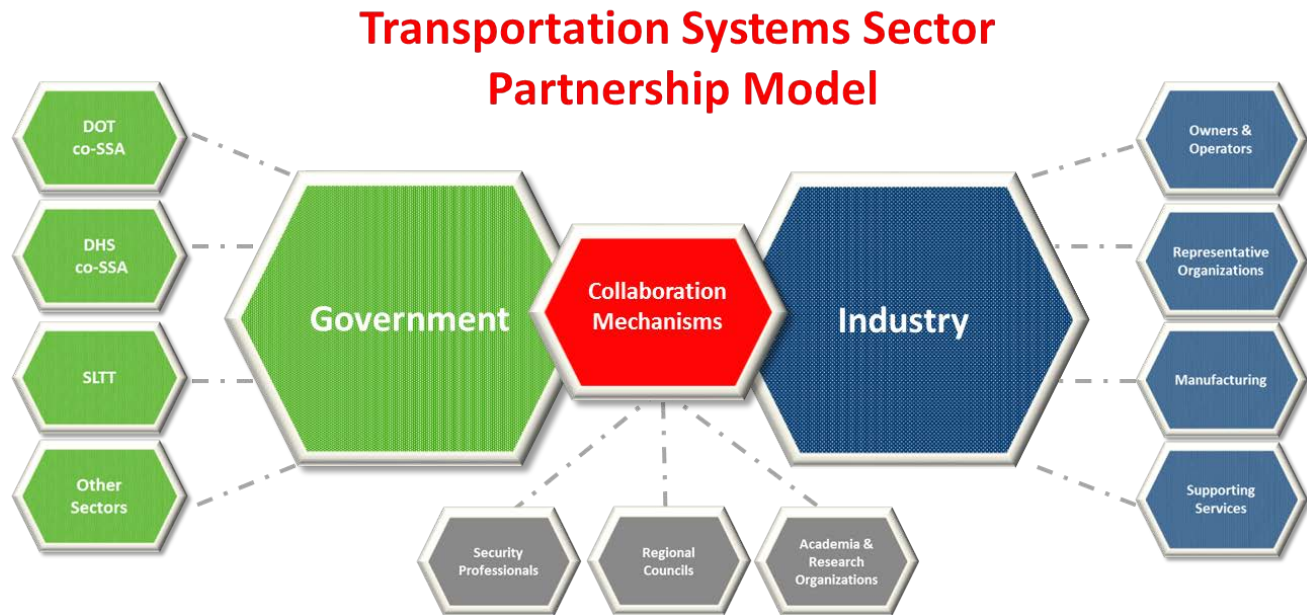
**Department of Transportation.** The DOT Office of Intelligence, Security, and Emergency Response oversees and administers DOT's co-SSA roles and responsibilities. The office coordinates closely with DOT's nine Operating Administrations, which directly manage the transportation programs that affect the security and resilience of critical transportation infrastructure. DOT's mission is to ensure a safe, efficient, and accessible transportation system that meets national interests and enhances the quality of life of the American people. DOT meets these challenges through grants, regulation, enforcement, research and development (R&D), and other means. Under the National Response Framework, DOT is the lead agency for coordinating Federal transportation activities during emergencies. In addition, DOT supports other agencies for response and recovery operations.

### 3.2.2 Management of Sector Responsibilities

The Sector co-SSAs are responsible for maintaining and updating the TS SSP collaboratively on a four-year cycle. The co-SSAs also lead the TS SSP annual review with Sector stakeholders. When updates are necessary, the co-SSAs work through the DHS Office of Infrastructure Protection (IP) to publish amendments or errata, as appropriate.

The co-SSAs annually evaluate progress implementing the TS SSP and report the progress to the DHS IP to support the development of the Critical Infrastructure National Annual Report.

Figure1: Transportation Systems Sector Partnership Model



### 3.2.3 The Sector Partnership

The NIPP 2013 Sector Partnership Model provides a mechanism for collaboration with public and private partners to promote the security and resilience of physical and cyber critical infrastructure. Federal and SLTT government partners contribute to Sector management through multiple forums. For example, Sector and subsector GCCs provide formal channels for government partners to advise the co-SSAs regarding cross-sector security and resilience dependencies, coordination of programs, and identification of capability gaps. GCCs also provide a gateway to receive advice from critical infrastructure owners and operators who are members of subsector (modal) SCCs.

The Sector Partnership Model also facilitates information exchanges between government representatives (Federal and SLTT) and critical infrastructure owners and operators, including through numerous conferences, meetings, workshops, and roundtables. The Secretary of Homeland Security established the Critical Infrastructure Partnership Advisory Council (CIPAC), in accordance with Section 201 of the Homeland Security Act of 2002, to allow industry to provide advice and consensus positions to the Federal Government. In recognition of the sensitive nature of the subject matter involved in CIPAC activities, the Secretary exempts CIPAC from the Federal Advisory Committee Act.<sup>4</sup>

The Sector co-SSAs have established joint working groups for collaboration in R&D and cybersecurity, and the co-SSAs are considering such groups for risk assessments and analyses, information sharing, and metrics. This partnership approach meets legislative requirements for collaboration among government and industry partners to ensure effective information exchange, set priorities, and develop effective solutions to protection and resilience risks (see Appendix C).

<sup>4</sup> Federal Advisory Committee Act of 1972

Information Sharing and Analysis Centers support the Sector and foster collaboration between government and private sector stakeholders. These partnership mechanisms allow for the protected flow of information between government and private stakeholders on a daily basis.

### **3.3 Cross-Sector Issues**

#### **3.3.1 Information Sharing**

A fundamental underpinning of public-private engagement is a commitment to ongoing information sharing. In the context of national resilience, the condition and functionality of transportation assets and infrastructure rest upon the fulfillment of this commitment. The Sector aims to bolster its national all-hazards resilience through continued attention to creating, integrating, and improving information sharing networks and practices.

The Sector's goals are consistent with those in the 2014 report to Congress on the Transportation Security Information Sharing Environment (TSISE), a plan required by the Intelligence Reform and Terrorism Prevention Act of 2004, as amended.

The goals listed in the TSISE include:

- Multi-directional sharing;
- Effective and efficient processes;
- Trusted partnerships;
- Security education, training, and awareness; and
- Protection of privacy and civil liberties.

The Sector requires an effective and efficient process for receiving, analyzing, and disseminating pertinent and timely threat and domain awareness information. The processes used in the Sector involve extensive communication within the Federal community and with public and private stakeholders. Effective protection or response relies on providing the stakeholders at greatest risk with real-time or near real-time alerts of emerging or breaking events. Accurate and up-to-date information distribution lists are an essential element of an effective process. To continually improve the performance of the Sector's information sharing mechanisms, the co-SSAs encourage stakeholders to critique information products and to contact the co-SSAs about areas for improvement.

At the Federal level, numerous information sharing channels provide public and private stakeholders with classified and unclassified briefings, assessments, and summaries. Stakeholders may report security concerns, safety issues, and suspicious incidents to the Federal Government through a number of hot lines or tip lines, such as:

- "If You See Something, Say Something™" Campaign (dial 911)
- General Aviation Security HOTLINE (1-866-427-3287)
- TSA Contact Center (1-866-289-9673)
- DOT Report Safety Violations (1-888-DOT-SAFT (368-7238))
- National Highway Traffic Safety Administration Hotline (1-888-DASH-2-DOT)
- USCG National Response Center Hotline (1-800-424-8802)

- America's Waterway Watch (877-24WATCH)
- First Observer™ Program (866-615-5150)

### **3.3.2 Cybersecurity**

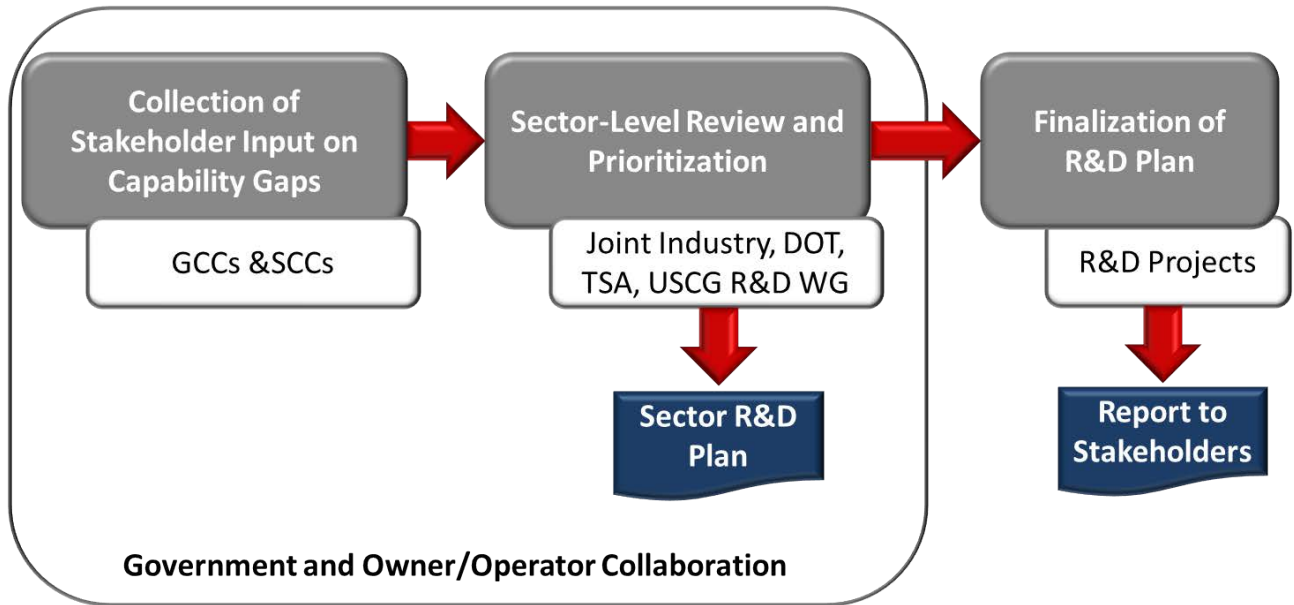
Cyber-based technologies in transportation operations enable greater economies and efficiencies, improve customer service, enhance operational controls, and provide better security capabilities. Consequently, transportation companies are increasingly dependent on cyber systems for business, security, and operational functions. Cyber technologies upon which transportation services rely include positioning, navigation, tracking, shipment routing, industrial system controls, access controls, signaling, communications, and data and business management. These technologies are often interconnected through networks and remote access terminals, which may allow malicious actors easier access to key nodes. Continuity of operations and system resilience following a disaster are increasingly dependent on the recovery of cyber systems.

### **3.3.3 Research and Development**

The Sector can enhance transportation security and resilience by identifying and applying existing and emerging technologies and processes that address current capabilities. Technology enhancements lead to operational efficiencies and often reduce costs. The Sector identifies gaps in security and resilience capabilities through aviation and surface R&D working groups. For example, the joint Surface Transportation Systems R&D Working Group, which includes representation from the co-SSAs and public and private sector partners, is the primary means of identifying capability gaps in the surface mode. The identified capability gaps are a basis for developing the R&D project requirements that the funding organization (e.g., DHS Office of Science and Technology (S&T), TSA, or DOT) will consider.

The Sector's R&D framework (Figure 2) describes the process by which the Sector's partners jointly identify and refine capability gaps and then submit their prioritized recommendations to funding organization for consideration in the budget process.

Figure 2: Sector Research and Development Framework



Within the maritime subsector, the USCG gathers gaps from across the USCG enterprise, which includes Coast Guard program offices that directly and indirectly support maritime subsector activities and frontline, port-level USCG operations officers. Research activities receive funding from several sources: the USCG R&D Program, components having equity in the maritime subsector, cooperative R&D agreements with maritime industry partners, S&T R&D partnerships, and the Homeland Security Advanced Research Projects Agency. DHS uses an assessment framework to prioritize projects based on potential impacts on risks.

## 4. Sector Goals and Priorities

The Sector’s partners identified the following goals and priorities in alignment with the NIPP 2013 and the JNPs (detailed in Appendix B).

**Sector Vision:** A secure and resilient transportation system, enabling legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties

**Sector Mission:** Continuously improve the security and resilience posture of the Nation’s transportation systems in order to ensure the safety and security of travelers and goods

Table 1: Sector Goals and Priorities

Sector Goals	Sector Priorities <sup>5</sup>
Goal 1: Manage the security risks to the physical, human, and cyber elements of critical transportation infrastructure	<ul style="list-style-type: none"> <li><b>A</b> Enhance the ability and the capacity to manage risks of terrorist attacks</li> <li><b>B</b> Advance the security posture of cyber systems essential for critical transportation operations</li> </ul>
Goal 2: Employ the Transportation Systems Sector response, recovery, and coordination capabilities to support whole community resilience	<ul style="list-style-type: none"> <li><b>C</b> Enhance critical transportation infrastructure preparedness for all-hazards resilience</li> <li><b>D</b> Support national credentialing program for access of emergency responders and infrastructure repair teams to areas impacted by disasters</li> <li><b>E</b> Expand partnerships to enhance resilience of communities and interdependent sectors</li> </ul>
Goal 3: Implement processes for effective collaboration to share mission essential information across sectors, jurisdictions, and disciplines and between public and private stakeholders	<ul style="list-style-type: none"> <li><b>F</b> Improve information sharing procedures for sustained awareness across sectors, jurisdictions, and disciplines and between public and private stakeholders</li> <li><b>G</b> Improve and expand partnerships to include interdependent sectors and SLTT partners</li> <li><b>H</b> Enhance transportation security and safety issue reporting, analysis, and dissemination through support of a nationwide reporting mechanism</li> </ul>
Goal 4: Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard U.S. national interests	<ul style="list-style-type: none"> <li><b>I</b> Expand risk-based security approaches, including risk segmentation, to securing and managing flows of people and goods into and out of the United States</li> <li><b>J</b> Promote global supply chain resilience</li> </ul>

<sup>5</sup> The priorities are mapped to the primary goals they support. However, the priorities and the activities supporting them could also support the accomplishment of other Sector goals, reflecting that the security and resilience missions are not isolated from each other, and counterterrorism activities are not isolated from activities for all-hazards preparedness.

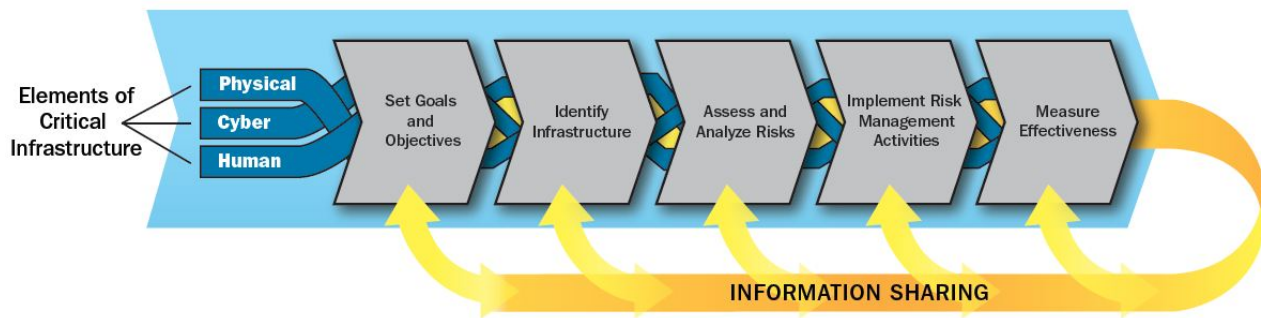


# 5. Achieving Sector Goals

## 5.1 Risk Management

Risk is the potential for an adverse outcome from an event, and is determined by the event’s threats, vulnerabilities, and consequences. The Sector assesses and manages security and resilience risks to physical and cyber transportation infrastructure and operations through a variety of methods and tools. These methods and tools support one or more of the steps in the NIPP RMF, the basis for Sector risk management—shown in Figure 3.

Figure 3: Critical Infrastructure Risk Management Framework (RMF)



The RMF depicts an approach to understanding and managing risk that invites sectors to identify and assess critical infrastructure (assets, systems, and networks) and to analyze the elements of risk (threats, vulnerabilities, and consequences) in order to determine risk-based priorities and risk management activities. At each step, RMF users should critique the processes they apply to inform future assessments and decisions and to improve the methods and tools used.

The size, complexity, and openness of the Sector, as well as the dynamic nature of threats and hazards, create challenges for risk managers, including:

- Uncertainties associated with the risks to the transportation system;
- Difficulties of predicting the likelihood and consequences of known risks;
- Inestimable nature of unknown threats;
- Wide spectrum of risks, often requiring different assessment methods and tools;
- Differences in risk assessment approaches for natural disasters and terrorism; and
- Varied preparedness and response capabilities and countermeasures within the modes.

The RMF assists resource managers and security officials to determine priorities, programs, and budgets for reducing risks from all hazards. As indicated in the RMF, the physical, cyber, and human elements of critical infrastructure are integral parts of transportation operations where risk management activities may be applied. Information sharing among security partners at each step of the RMF enhances the common basis for cohesive security and resilience planning.

### **5.1.1 Sector Interdependencies**

Transportation, energy, communications, and water are described in the NIPP 2013 as lifeline functions deemed essential to the operation of most sectors. Transportation assets and services are an important aspect of the security and resilience of other sectors and communities. The Sector depends on lifeline functions of other sectors. For example, maritime transportation relies on the Dams Sector for the function of locks and dams for river navigation, and it relies on the Information Technology Sector for voice and electronic data exchange related to cargo and passenger security. Examples of other sectors' dependence on transportation security and resilience include:

- The Chemical, Commercial Facilities, Critical Manufacturing, Defense Industrial Base, and Energy Sectors rely on transportation for the movement of raw materials, feed stocks, and products;
- The Commercial Facilities and Financial Services Sectors depend on postal and shipping to move essential paper transactions;
- The Emergency Services Sector depends on resilient transportation networks to respond effectively to emergencies;
- The Food and Agriculture Sector depends on the security of truck, rail, and maritime shipments to protect the Nation's food supply chain; and
- The Healthcare and Public Health Sector depends on transportation, particularly postal and shipping services, for delivery of medical supplies, medicines, and organs, often in urgent circumstances.

In addition to cross-sector dependencies, the Sector must pay particular attention to interdependencies among the transportation modes. For example, bridges and tunnels provide pathways for pipelines, mass transit, and railroads. In addition, many cyber systems, such as control systems or data centers, are shared between multiple transportation entities. Cyber attacks or other events that disrupt these systems could create consequences for critical infrastructure owners and operators across multiple modes. Furthermore, commodities may be shipped through multiple modes, which depend on one another for timely and secure deliveries to customers. These modal interdependencies require special consideration of the potential consequences from cascading effects of an incident.

### **5.1.2 Cybersecurity**

Cybersecurity risks are a growing and evolving challenge. The Sector's partners collaborate to plan for and counter cybersecurity threats. To the greatest extent possible, cybersecurity efforts are coordinated among DHS and DOT, which encourages unity of effort in cybersecurity initiatives and greater efficiency in evaluating the cyber threats, vulnerabilities, and consequences.

The principal cybersecurity partnership forum within the Sector is the Transportation Systems Sector Cybersecurity Working Group (TSSCWG), which includes Federal and SLTT government representatives as well as industry and private sector stakeholders. The TSSCWG builds on the Sector's 2012 Cybersecurity Strategy to manage risks by maintaining and enhancing awareness and promoting voluntary, collaborative, and sustainable community action.

The Sector's cybersecurity goals, as defined in the Strategy, are to:

- Maintain continuous cybersecurity awareness;
- Improve and expand voluntary participation in cybersecurity efforts;
- Define the conceptual environment;
- Enhance intelligence and security information sharing; and
- Ensure sustained coordination and strategic implementation.

In February 2013, EO 13636 set forth policies to address evolving cyber threats. Among other actions, the order directs the National Institute of Standards and Technology (NIST) to develop a Cybersecurity Framework, which NIST released in 2014. In 2015, the TSSCWG developed and distributed the Transportation Systems Sector Framework Implementation Guidance to help stakeholders assess and enhance their cybersecurity posture using the NIST Cybersecurity Framework.

The Guidance includes an information requirement that leverages ongoing work in DHS NPPD and the Federal Bureau of Investigation (FBI). DHS and the FBI have assisted hundreds of entities affected by cyber attacks, and they have discovered and shared hundreds of thousands of indicators from analyses of cyber incidents. Such analyses update cyber threat profiles in four fundamental areas:

- Tactics most commonly employed to gain illicit access to networks and systems;
- Vulnerabilities in targeted systems and networks most frequently exploited;
- Indicators of illicit cyber activities most often noted in post-incident analyses that were missed or disregarded; and
- Protective measures most often found lacking or absent that could have made a difference, aligned with the tactics these measures either defeat or mitigate.

In response to EO 13636, the Sector also assessed its critical cybersecurity functions and services to identify cyber-dependent infrastructure at greatest risk. Subject matter experts participated in the Cyber-Dependent Infrastructure Identification Working Group, led by DHS, to identify transportation assets where a cybersecurity incident could cause catastrophic results.

EO 13636 also directs DHS to establish a voluntary program to support the adoption of the NIST cybersecurity framework by critical infrastructure owners and operators. The Sector supports DHS' Critical Infrastructure Cyber Community Voluntary Program, which develops guidance for adoption of the NIST Cybersecurity Framework and the Enhanced Cybersecurity Services program. To facilitate a voluntary program, the DHS Office of Cybersecurity and Communications is working to identify no-cost cyber vulnerability assessment methodologies including:

- The Cyber Security Evaluation Program and Cyber Resilience Review process, a non-technical voluntary assessment for an organization to measure its cybersecurity capabilities against 10 domains.
- Cyber Infrastructure Survey Tool and Cyber Security Evaluation Tool, a voluntary technical assessment that exists as a downloadable application for an organization to assess the network infrastructure and components that support its control system operations and processes.

Congress requires the Government Accountability Office to report the progress implementing the voluntary adoption program.<sup>6</sup> The co-SSAs will contribute to the report on the extent to which such standards (1) are voluntary and led by industry representatives, (2) have been promoted by Federal agencies and adopted by sectors, and (3) have protected against cyber threats. The reports are to include the reasons sectors adopted or chose not to adopt the NIST standards.

### **5.1.3 Research and Development**

R&D activities are critical to developing state-of-the-art technologies and risk mitigation methodologies for transportation systems and networks. Research must focus on obstacle identification, innovative analysis, and capture of insights to develop creative approaches for issue resolution. Development needs to focus on tools, methodologies, and practices that are efficient, effective, and adaptable to diverse operations within the Sector.

Sector critical infrastructure owners and operators also lead R&D initiatives, sometimes in coordination with private sector partners. NIPP 2013 encourages R&D collaboration to bring the expertise and resources of public and private sector entities together for a common goal. For example, the USCG is currently working with electronic charting companies in cooperative research to evaluate risks to electronic navigation and aids to navigation.

The Critical Infrastructure Security and Resilience National R&D Plan (CISR R&D Plan),<sup>7</sup> required by PPD-21, was submitted to the President in February 2015 with five overarching priority areas that are intended to inform R&D investments, promote innovation, and guide research across the critical infrastructure communities:

- Develop foundational understanding of critical infrastructure systems and systems dynamics;
- Develop integrated and scalable risk assessment and management approaches;
- Develop integrated and proactive capabilities, technologies, and methods to support secure and resilient infrastructure;
- Harness the power of data sciences to create unified, integrated situational awareness and to understand consequences of action; and
- Build a cross-cutting culture of critical infrastructure security and resilience R&D collaboration.

The Sector will consider these five priority areas as inputs in its planning efforts to align R&D activities and support implementation of the National CISR R&D Plan.

## **5.2 Critical Infrastructure and National Preparedness**

PPD-21 specifically requires the sectors to align critical infrastructure security and resilience with PPD-8. The National Response Framework and the National Disaster Recovery Framework define DHS' and DOT's shared responsibilities for Federal transportation national preparedness.

---

<sup>6</sup> Cybersecurity Enhancement Act of 2014.

<sup>7</sup> <http://www.dhs.gov/publication/ncisr>. Accessed November 19, 2015.

The TS SSP aligns transportation disaster preparedness through the five National Preparedness System mission areas:

**Protection:** The Protection Mission Area applies to steady-state activities and includes safety and security programs aimed at reducing or managing risk to critical transportation infrastructure. In a non-terrorist incident or event, 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 suspects. Transportation stakeholders, particularly critical infrastructure owners and operators, have a responsibility to ensure the safety and security of the transportation infrastructure they operate.

**Prevention:** The Prevention Mission Area applies specifically to activities taken in response to an imminent terrorist attack. Although it is primarily a law enforcement mission, Sector stakeholders must be prepared to take additional precautionary steps to assist law enforcement as requested. Information sharing is critical to the success of this mission. 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 suspects.

**Mitigation:** The Mitigation Mission Area aims to reduce the consequence of an incident by identifying best practices as well as codes or standards that make transportation infrastructure more resilient. Mitigation activities can include building to standards that enhance resilience, identifying risks, ensuring additional protection measures are applied to reduce vulnerabilities, or taking actions to reduce the consequence of incidents that may occur. Mitigation activities are arguably best applied in the planning stage of infrastructure investment, but they can also be of value as complementary efforts to protection measures already undertaken. Properly applied mitigation efforts can reduce the vulnerability to, or consequence of, an incident while making response and recovery efforts easier.

**Response:** The Response Mission Area coordinates all response actions during a disaster to save lives and property at risk, and it conforms to the National Incident Management System, prescribed by Homeland Security Presidential Directive 5: Management of Domestic Incidents, and PPD-8. In addition, numerous DHS and DOT component agencies have specific statutory responsibilities for response and recovery efforts. During incident response, transportation capabilities support evacuations, rescue, medical care, and incident management.














**Recovery:** The Recovery Mission Area guides long-term recovery following an incident. The recovery phase begins when efforts to restore transportation infrastructure operations initiate. Transportation infrastructure is critical for facilitating response efforts, repair and restoration, and for supplying community needs during recovery efforts.

## 6. Measuring Effectiveness

The co-SSAs are responsible for supporting DHS statutorily required reporting requirements by providing Sector-specific critical infrastructure information on the effectiveness of security and resilience activities. The 2015 TS SSP identifies activities that include qualitative and quantitative approaches to measuring effectiveness. Responsible officials in government and industry should initiate measures of effectiveness and, as necessary, continuously improve the methodology, validity, accuracy, integrity, and reliability of each approach.

The activities listed in Table 2 are mapped to the primary priorities (listed on page 13) that they support. These activities can also support the accomplishment of other Sector priorities.

Table 2: Sector Activities and Measurement Approach

Maps to Sector Goal	Maps to Sector Priority	Sector Activity and Measurement Approach
 	 	<p><b>Sector Activity:</b> Include security and resilience plans—such as provisions for cybersecurity, awareness training, and periodic exercises—as a condition for receipt of security and resilience grants. (Modes with grant authorization)</p> <p><b>Measurement Approach:</b> FEMA to provide content data regarding security and resilience plan review for grant proposals.</p>
	 	<p><b>Sector Activity:</b> Jointly determine security, resilience, and cybersecurity capability gaps through the Sector’s collaborative R&amp;D prioritization processes. (All modes)</p> <p><b>Measurement Approach:</b> Qualitative assessment of the effectiveness of stakeholder participation in the R&amp;D processes.</p>
		<p><b>Sector Activity:</b> Identify and prioritize cyber-dependent critical infrastructure and systems. (All modes)</p> <p><b>Measurement Approach:</b> Progress completing identification and prioritization of cyber-dependent critical transportation infrastructure and systems.</p>
		<p><b>Sector Activity:</b> Encourage adoption of the NIST Cybersecurity Framework. (All modes)</p> <p><b>Measurement Approach:</b> Aggregate, non-attributional summary of voluntary reports on adoption of the NIST Cybersecurity Framework by transportation operators.</p>
		<p><b>Sector Activity:</b> Develop incentives to increase cybersecurity by:</p> <ul style="list-style-type: none"> <li>• Facilitating employee training opportunities;</li> <li>• Recognizing industry achievements in cybersecurity;</li> <li>• Certifying and confirming security measures as condition for grant award; and</li> <li>• Promoting participation in the DHS voluntary initiatives. (All modes)</li> </ul> <p><b>Measurement Approach:</b> Qualitative summary of actions taken in each mode. (All modes)</p>

Maps to Sector Goal	Maps to Sector Priority	Sector Activity and Measurement Approach
2	C	<p><b>Sector Activity:</b> Enhance critical transportation infrastructure preparedness for all hazards. (All modes)</p> <p><b>Measurement Approach:</b> Non-attributional, cumulative results of assessments of agencies and companies with high risk of terrorist attack.</p>
2	C	<p><b>Sector Activity:</b> Collaboratively identify and assess critical transportation infrastructure to manage risks and improve community resilience. (All modes)</p> <p><b>Measurement Approach:</b> Progress implementing scheduled infrastructure identification and assessment programs.</p>
2	D	<p><b>Sector Activity:</b> Provide a Sector-level forum for stakeholders to contribute to and participate in the DHS initiative to improve access to national disaster sites for response and recovery teams. (co-SSAs)</p> <p><b>Measurement Approach:</b> Progress meeting project timeline.</p>
2	E	<p><b>Sector Activity:</b> Improve relationships among Sector stakeholders at the transportation industry Chief Executive Officer, senior government, and SLTTGCC levels:</p> <ul style="list-style-type: none"> <li>• Facilitate Sector partnership through Sector and modal GCCs and SCCs. (co-SSAs)</li> <li>• Participate in senior-level CIPAC councils. (co-SSAs)</li> </ul> <p><b>Measurement Approach:</b> Qualitative assessment of participation in Sector Councils and member surveys.</p>
2	E	<p><b>Sector Activity:</b> Develop exercise injects to understand priorities for improving transportation resilience for highest threat scenarios. (All modes)</p> <p><b>Measurement Approach:</b> Trends showing numbers of exercises with transportation resilience objectives and persons participating in these exercises.</p>
2	E	<p><b>Sector Activity:</b> Support activities (exercises and operations) that build coordination and interoperability during responses and recovery operations. (All modes)</p> <p><b>Measurement Approach:</b> Trend showing change in coordination and interoperability based on joint exercises and operations.</p>
3	F	<p><b>Sector Activity:</b> Improve collaborative processes for effectively defining and improving security and resilience intelligence requirements. (All modes)</p> <ul style="list-style-type: none"> <li>• TSA engages with Federal, SLTT, and transportation industry stakeholders (maritime excluded) to validate transportation intelligence requirements, and shares these requirements with all transportation stakeholders as authorized.</li> </ul> <p><b>Measurement Approach:</b> Initial measure is amount of contact with different stakeholder groups within each transportation mode. Subsequent measure will be breadth of requirement dissemination.</p>

Maps to Sector Goal	Maps to Sector Priority	Sector Activity and Measurement Approach
3	F	<p><b>Sector Activity:</b> Create a collaborative process to identify information sharing capability gaps. (All modes)</p> <p><b>Measurement Approach:</b> A ratio of gaps identified to proposals submitted to DHS S&amp;T, and a second ratio of proposals submitted to DHS S&amp;T to those selected for R&amp;D projects.</p>
3	F	<p><b>Sector Activity:</b> Strengthen cybersecurity information sharing processes between subsector GCCs and SCCs.</p> <p><b>Measurement Approach:</b> Progress toward standing up subsector information sharing and analysis bodies.</p>
3	G	<p><b>Sector Activity:</b> Work with DHS to adjust the focus of Regional Resilience Assessment Program (RRAP) to capitalize on relationship-building potential. (All modes involved in RRAP)</p> <p><b>Measurement Approach:</b> Qualitative SLTT assessment of degree to which transportation related RRAPs have improved regional relationships among industry, government, communities, and emergency personnel.</p>
3	G	<p><b>Sector Activity:</b> Enhance engagement with States and regions at the field level through DHS' Captains of the Port, Protective Security Advisors, and Federal Security Directors; DOT's Regional Transportation Representatives; and Fusion Centers. (All modes)</p> <p><b>Measurement Approach:</b> Summation of record of specific actions taken to improve field force engagement in security and resilience mission.</p>
3	G	<p><b>Sector Activity:</b> DHS and DOT, through the GCCs and other partnering groups, engage other sectors and the SLTT partners to identify interdependencies and enhance efficient use of resources. (All modes, co-SSAs)</p> <p><b>Measurement Approach:</b> Qualitative assessment of the sufficiency of cross-sector engagements.</p>
3	H	<p><b>Sector Activity:</b> Define scope and approach in consultation with the transportation industry for an interagency solution and resourcing of a national tip-line that provides a single resource to address all-hazards incident and event reporting for the Sector. (Industry, co-SSAs)</p> <p><b>Measurement Approach:</b> Progress report relative to project timeline.</p>
3	H	<p><b>Sector Activity:</b> Update and share recommended practices and lessons-learned from assessments and exercises. (Industry, all modes)</p> <p><b>Measurement Approach:</b> Response to voluntary feedback questions disseminated through web survey, e-mail, and other media.</p>



Maps to Sector Goal	Maps to Sector Priority	Sector Activity and Measurement Approach
4	I	<p><b>Sector Activity:</b> Identify, assess, and prioritize efforts to manage supply chain risk using layered defenses in a changing security and operational environment. (DHS, Aviation, Maritime, Freight Rail)</p> <ul style="list-style-type: none"> <li>Integrate government and industry efforts to identify critical transportation elements of the global supply chain for vital commodities and movements.</li> </ul> <p><b>Measurement Approach:</b> Progress toward achieving comprehensive summary of supply chain risk management and resilience actions pertaining to transportation infrastructure.</p>
4	I	<p><b>Sector Activity:</b> Periodically assess supply chain security risks for all ports that ship cargo to the United States under the Cargo Security Initiative. (DHS)</p> <p><b>Measurement Approach:</b> Progress made in completing assessments.</p>
4	I	<p><b>Sector Activity:</b> Formalize information sharing arrangements between Federal agencies focused on cargo arriving and departing the United States, including law enforcement entities operating in the joint National Targeting Center for Cargo, and those agencies such as the Office of Naval Intelligence focused on cargo moving between foreign ports. (DHS)</p> <p><b>Measurement Approach:</b> Progress made by the joint National Targeting Center for Cargo and the Office of Naval Intelligence to document current mutual support practices and opportunities for improved cooperation.</p>
4	J	<p><b>Sector Activity:</b> Identify and address critical infrastructure supply chain cross-sector dependencies. (DHS, co-SSAs, dependent sectors)</p> <p><b>Measurement Approach:</b> Progress made in identifying transportation-related supply chain dependencies of other sectors.</p>
4	J	<p><b>Sector Activity:</b> Identify and use lessons learned from supply chain disruption events to inform policies and programs that enhance our Nation's preparedness. (DHS, co-SSAs)</p> <p><b>Measurement Approach:</b> Qualitative assessment of frequency and sufficiency of lessons-learned presented to decision makers.</p>
4	J	<p><b>Sector Activity:</b> Finalize standards for air cargo advance information requirements. (Aviation, CBP)</p> <p><b>Measurement Approach:</b> Progress toward delivering final standards.</p>

## Appendix A: Acronym List

CBP	U. S. Customs and Border Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CISR	Critical Infrastructure Security and Resilience
DHS	U.S. Department of Homeland Security
DOT	U.S Department of Transportation
EO	Executive Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GCC	Government Coordinating Council
IP	Office of Infrastructure Protection
JNP	Joint National Priorities
MSRAM	Maritime Security Risk Analysis Model
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NPPD	National Protection and Programs Directorate
PPD	Presidential Policy Directive
R&D	Research and Development
RMF	Risk Management Framework
RRAP	Regional Resilience Assessment Program
S&T	Science and Technology
SCC	Sector Coordinating Council
SLTT	State, local, tribal, and territorial
SSA	Sector-Specific Agency

TS SSP	Transportation Systems Sector-Specific Plan
TSA	Transportation Security Administration
TSISE	Transportation Security Information Sharing Environment
TSSCWG	Transportation Systems Sector Cybersecurity Working Group
TSSRA	Transportation Sector Security Risk Assessment
USCG	United States Coast Guard

# **Appendix B: Alignment with the NIPP 2013**

## **NIPP 2013 Goals**

1. Assess and analyze threats to, vulnerabilities of, and consequences to critical infrastructure to inform risk management activities;
2. Secure critical infrastructure against human, physical, and cyber threats through sustainable efforts to reduce risk, while accounting for the costs and benefits of security investments;
3. Enhance critical infrastructure resilience by minimizing the adverse consequences of incidents through advance planning and mitigation efforts, and employing effective responses to save lives and ensure the rapid recovery of essential services;
4. Share actionable and relevant information across the critical infrastructure community to build awareness and enable risk-informed decision making; and
5. Promote learning and adaptation during and after exercises and incidents.

## **NIPP 2013 Calls to Action**

1. Set National Focus through Jointly Developed Priorities
2. Determine Collective Actions through Joint Planning Efforts
3. Empower Local and Regional Partnerships to Build Capacity Nationally
4. Leverage Incentives to Advance Security and Resilience
5. Enable Risk-Informed Decision Making through Enhanced Situational Awareness
6. Analyze Infrastructure Dependencies, Interdependencies, and Associated Cascading Effects
7. Identify, Assess, and Respond to Unanticipated Infrastructure Cascading Effects During and Following Incidents
8. Promote Infrastructure, Community, and Regional Recovery Following Incidents
9. Strengthen Coordinated Development and Delivery of Technical Assistance, Training, and Education
10. Improve Critical Infrastructure Security and Resilience by Advancing Research and Development Solutions
11. Evaluate Progress toward the Achievement of Goals
12. Learn and Adapt During and After Exercises and Incidents

Table B-1: Contribution of Sector Priorities to Joint National Priorities and NIPP Goals

Joint National Priorities										
Transportation Sector Priorities	Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision Making	Share Information to Improve Prevention, Mitigation, Response, and Recovery	NIPP Goals				
						1	2	3	4	5
A. Enhance the ability and the capacity to manage risks of terrorist attacks	√	√			√	√	√	√		
B. Advance the security posture of cyber systems essential for critical transportation operations	√	√			√	√	√	√		
C. Enhance critical transportation infrastructure preparedness for all hazards	√	√	√	√		√	√	√		√
D. Support national credentialing program for access of emergency responders and infrastructure repair teams to areas impacted by disasters	√		√				√	√		√
E. Expand partnerships to enhance resilience of communities and interdependent sectors		√	√	√	√		√	√	√	

Joint National Priorities										
Transportation Sector Priorities	Strengthen Management of Cyber and Physical Risks to Critical Infrastructure	Build Capabilities and Coordination for Enhanced Incident Response and Recovery	Strengthen Collaboration Across Sectors, Jurisdictions, and Disciplines	Enhance Effectiveness in Resilience Decision Making	Share Information to Improve Prevention, Mitigation, Response, and Recovery Activities	NIPP Goals				
						1	2	3	4	5
F. Develop information sharing procedures for sustained awareness across sectors, jurisdictions, and disciplines and between public and private stakeholders		√	√		√	√			√	
G. Improve and expand partnerships to include interdependent sectors and SLTT partners	√	√	√	√	√			√	√	
H. Enhance transportation security and safety issue reporting, analysis, and dissemination through support of a nationwide reporting mechanism	√	√		√	√	√			√	
I. Expand risk-based security approaches, including risk segmentation, to securing and managing flows of people and goods into and out of the United States	√	√	√	√		√	√		√	√
J. Promote global supply chain resilience	√	√	√	√	√		√	√		√

Table B-2: Contribution of Sector Priorities to NIPP Call to Action

Transportation Sector Aligned Activities	NIPP 2013 Calls to Action											
	1	2	3	4	5	6	7	8	9	10	11	12
1. Include security and resilience plans—such as provisions for cybersecurity, awareness training, and periodic exercises—as a condition for receipt of security and resilience grants.	√	√	√	√					√			
2. Jointly determine security, resilience, and cybersecurity capability gaps through the Sector’s collaborative R&D prioritization processes.		√							√	√		
3. Identify and prioritize cyber dependent critical infrastructure and systems.		√				√	√	√				
4. Encourage adoption of the NIST Cybersecurity Framework.	√	√		√					√		√	
5. Develop incentives to increase cybersecurity.		√		√					√			√
6. Enhance critical transportation infrastructure preparedness for all hazards.	√	√			√		√	√	√		√	√
7. Collaboratively identify and assess critical transportation infrastructure to manage risks and improve community resilience.	√		√	√		√	√					
8. Provide a Sector-level forum for stakeholders to contribute to and participate in the DHS initiative to improve access to national disaster sites for response and recovery teams.	√	√	√		√		√	√				√
9. Improve relationships among Sector stakeholders at the transportation industry CEO, senior government, and SLTTGCC levels.	√	√	√		√							
10. Develop exercise injects to understand priorities for improving transportation resilience for highest threat scenarios.		√				√		√				√
11. Support activities (exercises and operations) that build coordination and interoperability during responses and recovery operations.		√	√		√	√	√				√	√
12. Improve collaborative processes for effectively defining and improving security and resilience intelligence requirements.	√	√			√		√					
13. Create a collaborative process to identify information sharing capability gaps.		√			√		√					√
14. Strengthen cybersecurity information sharing processes between subsector GCCs and SCCs.		√	√		√		√	√				

Transportation Sector Aligned Activities	NIPP 2013 Calls to Action											
	1	2	3	4	5	6	7	8	9	10	11	12
15. Work with DHS to adjust the focus of Regional Resilience Assessment Program (RRAP) to capitalize on relationship building potential.	√		√					√			√	
16. Enhance engagement with States and regions at the field level through DHS' Captains of the Port, Protective Security Advisors, and Federal Security Directors; DOT's Regional Transportation Representatives, and Fusion Centers.			√					√				
17. DHS and DOT engage other sectors and the SLTT partners through the GCCs and other partnering groups to identify interdependencies and enhance efficient use of resources.	√	√	√		√	√	√		√	√		
18. Define scope and approach in consultation with the transportation industry for an interagency solution and resourcing of a national tip-line that provides a single resource to address all-hazard incident and event reporting for the Sector.	√	√			√				√			
19. Update and share recommended practices and lessons-learned from assessments and exercises.	√	√	√				√		√		√	√
20. Identify, assess, and prioritize efforts to manage supply chain risk using layered defenses in a changing security and operational environment.	√	√				√	√				√	√
21. Periodically assess supply chain security risks for all ports that ship cargo to the United States under the Cargo Security Initiative.					√		√				√	√
22. Formalize information sharing arrangements between Federal agencies focused on cargo arriving and departing the United States., including law enforcement entities operating in the joint National Targeting Center for Cargo, and those agencies such as the Office of Naval Intelligence focused on cargo moving between foreign ports.					√						√	√
23. Identify and address critical infrastructure supply chain cross -sector dependencies.	√	√			√	√		√			√	√
24. Identify and use lessons-learned from supply chain disruption events to inform policies and programs that enhance our Nation's preparedness.			√		√						√	√
25. Finalize standards for air cargo advance information requirements.	√	√			√							√



# Appendix C: Authorities

The authorities for Federal responsibilities are found in various statutes, directives, and Executive Orders.

## Legislation

- Aviation and Transportation Security Act, Pub. L. 107-71 (Nov. 19, 2001)
- Homeland Security Act of 2002, Pub. L. 107-296 (Nov. 25, 2002)
- Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53 (Aug. 3, 2007)
- Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458 (Dec. 17, 2004)
- Maritime Transportation Security Act of 2002, Pub. L. 107-295 (Nov. 25, 2002)
- Post-Katrina Emergency Management Reform Act of 2006, Pub. L. 109-295 (Oct. 4, 2006)
- Security and Accountability For Every Port Act of 2006, Pub. L. 109-347 (Oct. 13, 2006)
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. 107-56 (Oct. 26, 2001)

## Executive Orders

- Executive Order 13636: Enhancing Critical Infrastructure Cybersecurity (Feb. 12, 2013)
- Executive Order 13416: Strengthening Surface Transportation Security (Dec. 5, 2006)

## Presidential Policy Directives

- Homeland Security Presidential Directive 5, Management of Domestic Incidents (Feb. 28, 2003)
- Presidential Policy Directive 8, National Preparedness (March 30, 2011)
- Presidential Policy Directive 21, Critical Infrastructure Security and Resilience (Feb. 12, 2013)

# Appendix D: Glossary of Terms

*Many of the definitions in this Glossary are from Federal laws, Executive or departmental directives, or the DHS Lexicon.*

**All Hazards.** A threat or an incident, natural or manmade, that warrants action to protect life, property, the environment, and public health or safety, and to minimize disruptions of government, social, or economic activities. It includes natural disasters, cyber incidents, industrial accidents, pandemics, acts of terrorism, sabotage, and destructive criminal activity targeting critical infrastructure. (Source: PPD-21, 2013)

**Asset.** Person, structure, facility, information, material, or process that has value. (Source: DHS Lexicon, 2010)

**Consequence.** The effect of an event, incident, or occurrence, including the number of deaths, injuries, and other human health impacts along with economic impacts both direct and indirect and other negative outcomes to society. (Source: Adapted from DHS Lexicon, 2010)

**Control Systems.** Computer-based systems used within many infrastructure and industries to monitor and control sensitive processes and physical functions. These systems typically collect measurement and operational data from the field, process and display the information, and relay control commands to local or remote equipment or human-machine interfaces (operators). Examples of types of control systems include Supervisory Control and Data Acquisition (SCADA) systems, Process Control Systems, and Distributed Control Systems. (Source: 2009 NIPP)

**Critical Infrastructure.** Systems and assets, whether physical or virtual, so vital to the United States. The incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (Source: §1016(e) of the USA Patriot Act of 2001 (42 U.S.C. §5195c(e))

**Critical Infrastructure Community.** Critical infrastructure owners and operators, both public and private; Federal departments and agencies; regional entities; SLTT governments; and other organizations from the private and nonprofit sectors with a role in securing and strengthening the resilience of the Nation's critical infrastructure and/or promoting practices and ideas for doing so. (Source: NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience*)

**Critical Infrastructure Information (CII).** Information that is not customarily in the public domain and is related to the security of critical infrastructure or protected systems. CII consists of records and information concerning any of the following:

- Actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law; harms the interstate commerce of the United States.; or threatens public health or
- The ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or

estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation, risk management planning, or risk audit.

- Any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, insurance, or continuity, to the extent that it is related to such interference, compromise, or incapacitation. (Source: CII Act of 2002, 6 U.S.C. § 131)

**Critical Infrastructure Owners and Operators.** Those entities responsible for day-to-day operation and investment of a particular critical infrastructure entity. (Source: Adapted from the 2009 NIPP)

**Critical Infrastructure Partnership Advisory Council (CIPAC).** Council established by DHS under 6 U.S.C. §451 to facilitate effective interaction and coordination of critical infrastructure activities among the Federal Government; the private sector; and SLTT governments. (Source: CIPAC Charter)

**Critical Infrastructure RMF.** A planning, decision-making, and risk management framework that outlines the process for setting goals and objectives, identifying infrastructure, assessing risks, implementing risk management activities, and measuring effectiveness to inform continuous improvement in critical infrastructure security and resilience. (Source: Adapted from the 2009 NIPP)

**Cybersecurity.** The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wireline, wireless, satellite, public safety answering points, and 911 communications systems and control systems. (Source: 2009 NIPP)

**Cyber System.** Any combination of facilities, equipment, personnel, procedures, and communications integrated to provide cyber services; examples include business systems, control systems, collision avoidance systems, SCADA systems, fire suppression systems, industrial control systems, signals and access control systems. (Source: 2009 NIPP)

**Executive Order 13636.** Executive Order that calls for the Federal Government to closely coordinate with critical infrastructure owners and operators to improve cybersecurity information sharing; develop a technology-neutral cybersecurity framework; and promote and incentivize the adoption of strong cybersecurity practices. (Executive Order 13636,17 Improving Critical Infrastructure Cybersecurity, February 2013)

**Federal Advisory Committees (FACs).** As used in the TS SSP, FACs are advisory groups managed under legislative authority to provide private sector advice to the Federal Government. Examples of FACs include, but are not limited to, the Aviation Security Advisory Committee, the National Maritime Security Advisory Committee, the CIPAC, the National Freight Advisory Committee, and the Rail Transit Safety Advisory Committee.

**Federal Departments and Agencies.** Any component of the United States Government that is an “agency” under 44 U.S.C. §3502(1) other than those considered to be independent regulatory agencies as defined in 44 U.S.C. §3502(5). (Source: PPD-21, 2013)

**Fusion Center.** A State and major urban area focal point for the receipt, analysis, gathering, and sharing of threat-related information between the Federal Government, SLTT, and private sector partners. (Source: Adapted from the DHS Lexicon, 2010)

**Government Coordinating Council (GCC).** The government counterpart to the Sector Coordinating Council for each sector, established to enable interagency and intergovernmental coordination; comprises representatives across various levels of government (Federal and SLTT) as appropriate to the risk and operational landscape of each sector. (Source: 2009 NIPP)

**Hazard.** Natural or manmade source or cause of harm or difficulty. (Source: DHS Lexicon, 2010)

**Incident.** An occurrence, caused by either human action or natural phenomenon, that may cause harm and require action, which can include major disasters, emergencies, terrorist attacks, terrorist threats, wild and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, cyber attacks, cyber failure/accident, and other occurrences requiring an emergency response. (Source: DHS Lexicon, 2010)

**Information Sharing and Analysis Centers (ISACs).** Entities formed by critical infrastructure owners and operators to gather, analyze, appropriately sanitize, and disseminate intelligence and information related to critical infrastructure. ISACs provide 24/7 threat warning and incident reporting capabilities and have the ability to reach and share information within their sectors, between sectors, and among government and private sector stakeholders. (Source: Presidential Decision Directive 63, 1998)

**Infrastructure.** The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures), and distribution capabilities that provide a reliable flow of products and services essential to the defense and economic security of the United States., the smooth functioning of government at all levels, and society as a whole; consistent with the definition in the Homeland Security Act, infrastructure includes physical, cyber, and/or human elements. (Source: DHS Lexicon, 2010)

**Interdependency.** Mutually reliant relationship between entities (objects, individuals, or groups); the degree of interdependency does not need to be equal in both directions. (Source: DHS Lexicon, 2010)

**Mitigation.** Capabilities necessary to reduce loss of life and property by lessening the impact of disasters. (Source: PPD-8, 2011)

**Network.** A group of components that share information or interact with each other to perform a function. (Source: 2009 NIPP)

**Partnership.** Close cooperation between parties having common interests in achieving a shared vision. (Source: NIPP 2013)

**Presidential Policy Directive 8 (PPD-8).** Facilitates an integrated, all-of-Nation approach to national preparedness for the threats that pose the greatest risk to the security of the Nation,

including acts of terrorism, cyber attacks, pandemics, and catastrophic natural disasters; directs the Federal Government to develop a national preparedness system to build and improve the capabilities necessary to maintain national preparedness across the five mission areas covered in the PPD: prevention, protection, mitigation, response, and recovery. (Source: PPD-8, 2011)

**Presidential Policy Directive 21 (PPD-21).** Aims to clarify roles and responsibilities across the Federal Government and establish a more effective partnership with critical infrastructure owners and operators and SLTT entities to enhance the security and resilience of critical infrastructure. (Source: PPD-21, 18 2013)

**Prevention.** Those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. (Source: PPD-8, 2011)

**Protection.** Those capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters. (Source: PPD-8, 2011)

**Recovery.** Those capabilities necessary to assist communities affected by an incident to recover effectively, including, but not limited to, rebuilding infrastructure systems; providing adequate interim and long-term housing for survivors; restoring health, social, and community services; promoting economic development; and restoring natural and cultural resources. (Source: PPD-8, 2011)

**Regional.** Entities and interests spanning geographic areas ranging from large multi-State areas to metropolitan areas and varying by organizational structure and key initiatives, yet fostering engagement and collaboration between critical infrastructure owners and operators, government, and other key stakeholders within the given location. (Source: *Regional Partnerships: Enabling Regional Critical Infrastructure Resilience, RC3, March 2011*)

**Resilience.** The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions; includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. (Source: PPD-21, 2013)

**Response.** Capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred. (Source: PPD-8, 2011)

**Risk.** The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences. (Source: DHS Lexicon, 2010)

**Risk-Informed Decision Making.** The determination of a course of action predicated on the assessment of risk, the expected impact of that course of action on that risk, and other relevant factors. (Source: 2009 NIPP)

**Sector.** A logical collection of assets, systems, or networks that provide a common function to the economy, government, or society; the *National Plan* addresses 16 critical infrastructure sectors, as identified in PPD-21. (Source: Adapted from the 2009 NIPP)

**Sector Coordinating Council (SCC).** The private sector counterpart to the GCC, these councils are self-organized, self-run, and self-governed organizations that are representative of a spectrum

of key stakeholders within a sector; serve as principal entry points for the government to collaborate with each sector for developing and coordinating a wide range of critical infrastructure security and resilience activities and issues. (Source: Adapted from the 2009 NIPP)

**Sector Partners.** As used in the TS SSP, sector partners are Federal and SLTT government entities and critical infrastructure owners and operators of critical infrastructure who have primary responsibilities for planning and programming the security and resilience of the transportation system.

**Sector-Specific Agency (SSA).** A Federal department or agency designated by PPD-21 with responsibility for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment. (Source: PPD-21, 2013)

**Sector-Specific Plans (SSP).** Planning documents that complement and tailor application of the *National Plan* to the specific characteristics and risk landscape of each critical infrastructure sector; developed by the SSAs in close collaboration with the SCCs and other sector partners. (Source: Adapted from the 2009 NIPP)

**Secure/Security.** Reducing the risk to critical infrastructure by physical means or defensive cyber measures to intrusions, attacks, or the effects of natural or manmade disasters. (Source: PPD-21, 2013)

**Steady State.** The posture for routine, normal, day-to-day operations as contrasted with temporary periods of heightened alert or real-time response to threats or incidents. (Source: DHS Lexicon, 2010)

**System.** Any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose. (Source: DHS Lexicon, 2010)

**Terrorism.** Premeditated threat or act of violence against noncombatant persons, property, and environmental or economic targets to induce fear, intimidate, coerce, or affect a government, the civilian population, or any segment thereof, in furtherance of political, social, ideological, or religious objectives. (Source: DHS Lexicon, 2010)

**Threat.** A natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. (Source: DHS Lexicon, 2010)

**Vulnerability.** A physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. (Source: DHS Lexicon, 2010)