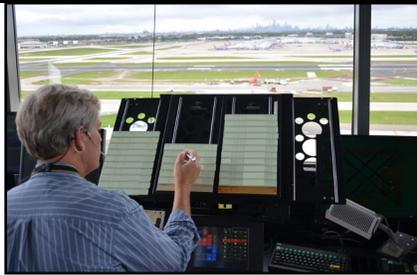


2018

Transportation Systems Sector Activities Progress Report



**Homeland
Security**



United States
Department of Transportation

TABLE OF CONTENTS

ABOUT THE TRANSPORTATION SYSTEMS SECTOR..... 1

PREFACE 2

2018 TRANSPORTATION SYSTEMS SECTOR GOALS PROGRESS REPORT..... 3

EXECUTIVE SUMMARY 4

OVERVIEW OF SECTOR PROGRESS 6

Sector Strengths 6

Opportunities to Increase Sector Goal Achievement..... 7

Recommendations..... 9

METHODOLOGY FOR PROGRESS MEASUREMENT OF SECTOR ACTIVITIES 10

GOAL 1 – “MANAGE THE SECURITY RISKS TO PHYSICAL, HUMAN, AND CYBER ELEMENTS OF CRITICAL TRANSPORTATION INFRASTRUCTURE.” 11

GOAL 2 – “EMPLOY THE TRANSPORTATION SYSTEMS SECTOR RESPONSE, RECOVERY, AND COORDINATION CAPABILITIES TO SUPPORT WHOLE COMMUNITY RESILIENCE.”..... 14

GOAL 3 – “IMPLEMENT PROCESSES FOR EFFECTIVE COLLABORATION TO SHARE MISSION ESSENTIAL INFORMATION ACROSS SECTORS, JURISDICTIONS, AND DISCIPLINES AND BETWEEN PUBLIC AND PRIVATE STAKEHOLDERS..... 17

GOAL 4 – “ENHANCE THE ALL-HAZARDS PREPAREDNESS AND RESILIENCE OF THE GLOBAL TRANSPORTATION SYSTEM TO SAFEGUARD U.S. NATIONAL INTERESTS. 20

PRIVATE SECTOR PACESETTERS 23

APPENDIX A: ACRONYMS AND REFERENCES LIST 25

APPENDIX B: TRANSPORTATION SYSTEMS SECTOR ACTIVITY SUMMARY REPORTS..... 28

APPENDIX C: GLOSSARY OF TERMS 58

About the Transportation Systems Sector

Presidential Policy Directive (PPD)-21, *Critical Infrastructure Security and Resilience*, names 16 critical infrastructure sectors and the executive departments responsible for overseeing security and resilience in each sector. The directive designates the U.S. Department of Homeland Security (DHS) and the U.S. Department of Transportation (DOT) as Co-Sector Specific Agencies (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).

The Transportation Systems Sector (Sector) consists of seven key subsectors, or modes: aviation, highway and motor carrier, maritime transportation system, mass transit and passenger rail, pipeline systems, freight rail, and postal and shipping. The Sector is responsible for the security and resilience of the Nation's transportation system, supporting the system's ability to quickly, safely, and securely move people and goods throughout the country and overseas.

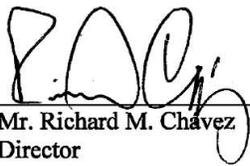
Preface

As Co-SSAs for the Transportation Systems Sector, DHS—with TSA and the USCG as its executive agents—and DOT drafted the 2018 Transportation Systems Sector Activities Progress Report.

In 2015, DHS and DOT jointly published the Transportation Systems Sector Specific Plan (TS SSP)¹ in collaboration with Sector partners. The Plan defined the roles and responsibilities of government and the private sector, and proposed goals, priorities, and activities to manage risks and contribute to the national security and resilience goals in the National Infrastructure Protection Plan (NIPP) 2013.² Additionally, the Plan identified the Sector’s mission 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.” Co-SSAs have tracked activity progress since the publication of the TS SSP and drafted activity summary reports to highlight work accomplished for each activity. Detailed activity summary reports are included in [Appendix B](#) of this report.

The content of the report and measurement of progress toward TS SSP goals and activities reflects Co-SSA efforts, drawn from the Co-SSA activity summary reports. This report does not capture TS SSP activity-related security and resilience initiatives carried out by public and private sector stakeholders, aside from activities which included direct engagement from Co-SSA representatives. Co-SSAs will use this report to communicate to public and private sector stakeholders the current measurement of Co-SSA progress toward each Sector goal. However, going forward, Co-SSAs hope that this report will serve as a starting point to engage with public and private sector partners to better understand and capture their progress toward Sector goals and to collaborate in determining future Sector priorities.

This report also identifies Sector gaps in completing described activities and maps out projected milestones and next steps for Sector stakeholders to take over the course of the next five years. Next steps aligned to Sector goals are not intended to be prescriptive and should subsequently be collaborated and expanded upon across all Sector stakeholders. Sector partners—who share responsibility for continuously improving the security and resilience of transportation systems and assets—are highly encouraged to contribute to the overall recommendations and goal-specific next steps provided in this report and to propose alternate courses of action.



Mr. Richard M. Chavez
Director
Office of Intelligence, Security, and
Emergency Response (S-60)
U.S. Department of Transportation



Mr. Eddie D. Mayenschein
Assistant Administrator
Policy, Plans, and Engagement
Transportation Security Administration



RADM J. P. Nadeau
Assistant Commandant for Prevention Policy
U.S. Coast Guard

¹ [Link to the 2015 Transportation Systems Sector Activities Report – https://www.dhs.gov/publication/nipp-ssp-transportation-systems-2015.](https://www.dhs.gov/publication/nipp-ssp-transportation-systems-2015)

² [Link to the 2013 National Infrastructure Protection Plan – https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience](https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience)

Overall Progress Score: 3.6

Goal	Average Activity Score
------	------------------------



Manage the security risks to physical, human, and cyber elements of critical transportation infrastructure.



Employ the Transportation Systems Sector response, recovery, and coordination capabilities to support whole community resilience.



Implement processes for effective collaboration to share mission essential information across sectors, jurisdictions, and disciplines and between public and private stakeholders.



Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard U.S. national interests.



Executive Summary

The purpose of the 2018 Transportation Systems Sector Activities Progress Report is to assess Sector progress toward TS SSP goal achievement based on Sector activities commenced or completed by co-SSAs, and to provide a recommended direction for the Sector to continue to evolve the security and resilience of the national transportation system and assets.

The report reveals that the Sector made substantial advancement on most Sector activities, but ample opportunity remains for further achievement and expansion of Sector work supporting each of the four Sector goals. The report also acknowledges that, over the past three years, Sector work has not adequately leveraged stakeholder networks and resources to their fullest capacity, especially concerning private sector partner engagement. Going forward, the Sector will explore how to better connect the public and private sector networks to more efficiently and effectively accomplish current and future activities. Increasing and diversifying the Sector's security and resilience portfolio and enhancing its public-private partnerships will better serve the Sector as it faces growing threats, new technology, and aging infrastructure.

Evaluated on a scale of 1 to 5, with a score of 5 indicating a completed goal and a score of 1 indicating no goal progress, Sector goal scores ranged from a 3.2 to a 4.0. The score of each goal was calculated by averaging the scores of all goal-aligned activities originally provided in the TS SSP.

The Sector's activities were drawn from four focal points: information sharing, cybersecurity, R&D, and critical infrastructure and national preparedness. Consequently, these focal points were absorbed as strengths by the Sector, although there is still room for growth and transformation.

5 Goal Complete

The Sector met all requirements initially proposed in the TS SSP for all activities aligned to the goal. The work completed for the activities supported achievement of one or more priorities provided for the overarching Sector goal. The goal will be assessed for alternative application to future Sector needs.

4 Substantial Goal Achievement

The Sector met the majority of requirements initially proposed in the TS SSP for all or most activities aligned to the goal, however, all requirements were not met. The goal may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activities supported achievement of one or more priorities provided for the overarching Sector goal.

3 Partial Goal Achievement

The Sector met less than the majority of requirements initially proposed in the TS SSP for all or most activities aligned to the goal. Sector activities progress, to date, has not supported achievement of one or more priorities provided for the overarching Sector goal.

2 Goal Work Initiated

The Sector initiated work toward the requirements initially proposed in the TS SSP for at least one activity aligned to the goal, however, no requirements for any aligned goal activity have been achieved. Sector activities progress, to date, has not supported achievement of one or more priorities provided for the overarching Sector goal.

1 No Goal Progress

The Sector has not initiated work toward the requirements initially proposed in the TS SSP for the aligned goal activities. Sector activities progress, to date, has not supported achievement of one or more priorities provided for the overarching Sector goal.

Gaps in Sector involvement were illustrated in five areas after evaluating work completed for each activity: private sector engagement, modal dependencies and interdependencies, supply chain resilience, exercise integration, and intersections with international programs.

The following recommendations offer a practical and progressive way for the Sector to better its approach to enhance the security and resilience posture of the Nation's transportation systems:

Recommendation 1 – Eliminate obsolete Sector activities and revise Sector goals and activities to reflect new Sector priorities

Many of the Sector activities were completed or are nearing completion. Sector activities should be vetted and updated to include the new Sector priorities and the proposed five focus areas shared below in Recommendation 2.

Recommendation 2 – Increase Sector engagement across the following five proposed focus areas: private sector engagements, modal dependencies and interdependencies, supply chain resilience, exercise integration, and intersections with international programs

The Sector should continue to support and expand its work regarding: information sharing, cybersecurity, R&D, and critical infrastructure and national preparedness. However, introducing these proposed five focus areas will strengthen the Sector's portfolio through: (1) increasing involvement from the private sector, which owns and oversees many transportation systems and assets, and (2) expanding the Sector's scope of work to advance security and resilience for national and global transportation networks and supply chains and for national emergency management.

Recommendation 3 – Create Sector milestones to promote activity and goal achievement

Revised Sector goals and activities should be aligned with clear milestones to guide the Sector on a definitive timeline that empowers all stakeholders to work toward activity and goal achievement.

Recommendation 4 – Create a practical and effective progress measurement system for activities, and capture public and private sector partner achievements

The activity measurement approaches provided in the TS SSP 2015 did not adequately assess progress made toward Sector goals and aligned activities. Improved measurement approaches that provide a simple and effective means to track Sector progress should be established and aligned with future activities. Although the Sector tracked goal progress completed by Co-SSA engagement, public and private sector stakeholder efforts were not formally tracked by Co-SSAs. Moving forward the Sector should comprehensively capture Co-SSA efforts and public and private Sector partner efforts.

Overview of Sector Progress

The Sector received an overall progress score of 3.6 for its work on goal activities, measured by averaging the four overall goal scores. The Sector made progress in work related to information sharing, cybersecurity, R&D, and critical infrastructure and national preparedness across all seven key subsectors. These four focus areas translated into Sector strengths due to the extent of activity pursued by public and private sector stakeholders. These focus areas are vital to maintaining and elevating the Sector's security and resilience posture as Sector networks expand and overlap, cyber technology is further integrated into transportation systems, and natural and manmade disasters increase in quantity and impact.

Sector Strengths

Information Sharing

The Sector bolstered its national all-hazards resilience mission through its continued attention to creating, integrating, and improving information sharing networks and practices. The Sector's commitment to ongoing information sharing serves as a fundamental underpinning of public-private engagement. In the context of national resilience, the condition and functionality of transportation assets and infrastructure rests upon fulfilling this commitment.

Cybersecurity

The Sector identified cyber support networks and resources, educated stakeholders on cybersecurity initiatives, and advanced the development of sector-specific cybersecurity resources. 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. Transportation services rely on cyber technology, including 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.

Research and Development

The Sector supported the development and deployment of tools, training, and other assistance to enhance preparedness and resilience. Technology enhancements lead to operational efficiencies and often reduce costs. The Sector identified gaps in security and resilience capabilities through aviation and surface R&D working groups. The identified capability gaps serve as a basis for developing the R&D project requirements that the funding organization may consider for award recipients.

Critical Infrastructure and National Preparedness

PPD-21 requires sectors to align critical infrastructure security and resilience with PPD-8, *National Preparedness*. In addition, the National Response Framework (NRF) and the National Disaster Recovery Framework define DHS- and DOT-shared responsibilities for federal transportation national preparedness. Through addressing the five National Preparedness System mission areas—protection, prevention, mitigation, response, and recovery—the Sector took steps to enhance critical transportation infrastructure. The Sector—built upon existing processes and relationships, used lessons learned from operations and exercises to strengthen Sector all-hazards response, honed its skill set and resources to address cybersecurity needs, and increased cross-sector collaboration.

Opportunities to Increase Sector Goal Achievement

Opportunities for Sector growth remain in the areas of information sharing, cybersecurity, R&D, and critical infrastructure and national preparedness. In addition, the Sector exhibits strong potential for diversifying its portfolio and influence in the following subject areas:

Private Sector Engagement

The private sector can voluntarily collaborate with the government to establish priorities and coordinate activities related to Sector critical infrastructure security and resilience. Private sector participation is essential to achieving optimal Sector effectiveness and efficiency. The private sector has made significant strides in critical infrastructure security and resilience, often implementing leading edge and innovative solutions. However, as a Sector, we have not fully leveraged private sector expertise and resources to support achieving current goals and expanding our reach to the most relevant security and resilience needs across all modes.

As owners and operators of a large portion of the Sector’s critical infrastructure, the private sector is primarily responsible for critical infrastructure security and resilience. The private sector conducts risk assessments, develops plans, implements risk management programs, and conducts training and exercises to enhance critical infrastructure security and resilience. Going forward, the Co-SSAs aim to fortify communication processes with private stakeholders and will identify how they can better serve the needs of the private sector through support and resources.

Modal Dependencies and Interdependencies

The TS SSP stresses identifying and assessing existing dependencies and interdependencies between all 16 critical infrastructure sectors. Dependencies and interdependencies across all modes of transportation have not been wholly implemented into Sector goals, priorities or activities. Addressing dependencies and interdependencies would involve mapping the Transportation Systems ecosystem, identifying intertwined vulnerabilities, and developing, implementing, and enhancing the practical strategies to mitigate cascading consequences of attacks.

Supply Chain Resilience

Global and national supply chains are attractive targets for terrorist attacks and criminal exploitation and remain vulnerable to natural disasters. The global supply chain relies on an interconnected web of transportation infrastructure pathways. The Sector's vision and mission underline a shared responsibility to "enable legitimate travelers and goods to move without significant disruption of commerce, undue fear of harm, or loss of civil liberties" and to "ensure the safety and security of travelers and goods." To create a secure and resilient transportation system and supply chain, the Sector needs to (1) refine its understanding of threats and risks to the global supply chain system as an interconnected network, (2) encourage its stakeholders to build resilience into the supply chains that their transportation systems and assets support, and (3) map interdependencies among supported supply chains with other overlapping critical infrastructure sectors.

Exercise Integration

The Sector minimizes disruption to its critical infrastructure functions through incident response preparation, planning, and exercising. Flexibility and adaptability to incorporate new information; such as, a changing risk environment, lessons learned, and best practices, serve as the core of preparedness and planning exercises. Sector engagement, during exercises and incidents, can be broadened to: (1) assist stakeholders with adapting exercise programs and training to capture Sector priorities, (2) include a wider range of Sector and cross-sector participants, (3) collect resources and tools for exercise development, and (4) share exercise findings and real-world trends for future use.

Intersections with International Programs

Most public and private sector stakeholders are either directly engaged with, or inadvertently affected by, international partners and influence on national transportation systems and assets. Sector work primarily serves nationally-focused and sourced efforts, but this leaves an untapped network of international partnerships, information sharing, best practices, and additional resources. Including international engagement into future Sector work will promote solutions to integrated global multimodal transportation issues, advocacy in transportation security and resilience, international technical assistance and cooperation, and contributing to transportation policy development related to security and resilience.

Recommendations

The following recommendations address a practical and progressive approach for the Sector to continue its mission to improve the security and resilience posture of the Nation's transportation systems:

Recommendation 1 – Eliminate obsolete Sector activities and revise Sector goals and activities to reflect new Sector priorities

Many of the Sector activities were completed or are nearing completion. Sector activities should be vetted and updated to include the new Sector priorities and the proposed five focus areas shared below in Recommendation 2.

Recommendation 2 – Increase Sector engagement across the following five proposed focus areas: private sector engagements, modal dependencies and interdependencies, supply chain resilience, exercise integration, and intersections with international programs

The Sector should continue to support and expand its work regarding: information sharing, cybersecurity, R&D, and critical infrastructure and national preparedness. However, introducing these proposed five focus areas will strengthen the Sector's portfolio through: (1) increasing involvement from the private sector, which owns and oversees many transportation systems and assets, and (2) expanding the Sector's scope of work to advance security and resilience for national and global transportation networks and supply chains and for national emergency management.

Recommendation 3 – Create Sector milestones to promote activity and goal achievement

Revised Sector goals and activities should be aligned with clear milestones to guide the Sector on a definitive timeline that empowers all stakeholders to work toward activity and goal achievement.

Recommendation 4 – Create a practical and effective progress measurement system for activities, and capture public and private sector partner achievements.

The activity measurement approaches provided in the TS SSP 2015 did not adequately assess progress made toward Sector goals and aligned activities. Improved measurement approaches that provide a simple and effective means to track Sector progress should be established and aligned with future activities. Although the Sector tracked goal progress completed by Co-SSA engagement, public and private sector stakeholder efforts were not formally tracked by Co-SSAs. Moving forward the Sector should comprehensively capture Co-SSA efforts and public and private Sector partner efforts.

This report marks the first comprehensive assessment of the Sector’s goal and activities achievement to date. The TS SSP outlined Sector priorities for each goal and proposed a means of measurement for activities under each goal. A definitive methodology for evaluating and measuring goal and activity progress, however, was not established in the TS SSP. Therefore, to create a baseline for the evaluation of activity progress and to assist the Sector in achieving its goals, the following simple scoring criteria was established to evaluate each activity on a scale of 1 to 5:

Activity Scoring Scale

5: Activity Complete

The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported the achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

4: Substantial Activity Achievement

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however, all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported the achievement of one or more priorities provided for its overarching Sector goal.

3: Partial Activity Achievement

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported the achievement of one or more priorities provided for its overarching Sector goal.

2: Activity Work Initiated

The Sector initiated work toward the requirements initially proposed in the TS SSP for the activity, however, no requirements have been achieved. Sector activity progress, to date, has not supported the achievement of one or more priorities provided for its overarching Sector goal.

1: No Activity Progress

The Sector has not initiated work toward the requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported the achievement of one or more priorities provided for its overarching Sector goal.

An average score of each goal’s activities was calculated to provide a score for overall goal achievement. Each activity summary and accompanying score and calculation can be found in [Appendix B](#). The Sector will look to evaluate current and future activities to determine applicable and consistent means of measurement following the release of this report and through stakeholder feedback.

Goal 1 – “Manage the security risks to physical, human, and cyber elements of critical transportation infrastructure.”

GOAL 1

Average Score: 3.6

Activity

Score



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.



Jointly determine security, resilience, and cybersecurity capability gaps through the Sector’s collaborative R&D prioritization process.



Identify and prioritize cyber dependent critical infrastructure systems.



Encourage adoption of the NIST Cybersecurity Framework.



Develop incentives to increase cybersecurity.



Overview

Goal 1 is composed of five activities that focus on managing security risks to physical, human, and cyber elements of critical transportation infrastructure. In its approach to achieve activity progress, the Sector placed a strong emphasis on advancing cybersecurity to mitigate cyber risk and residual risk to physical human elements. Sector improvements and incentives in security training and exercises increased security management through R&D prioritization and planning. The Sector received an average score of 3.6. for Goal 1.

Highlights

DHS revised existing DHS security grants for content inclusion of mandatory security and resilience requirements. Many revised grants were port and transit security grants, provisioned through the Federal Emergency Management Agency (FEMA). Along with grant revisions, DHS assessed its existing R&D prioritization of investments to pinpoint gaps in security, resilience, and cybersecurity. DHS's Office of Science & Technology (S&T) gathered public and private surface transportation stakeholder input through the Critical Infrastructure Partnership Advisory Council (CIPAC), Transportation Systems Sector (TSS) Research and Development Working Group (RDWG) for consideration in reprioritizing R&D investments. DOT contributed through the CIPAC TSS RDWG and serving as a member of DHS's "Enhance Security" sub-Integrated Product Team (IPT), chaired by TSA. IPT members provided collaboration regarding security topics and helped to identify technology capability gaps. The resulting annual DHS IPT R&D Fiscal Year (FY) 16 and FY 17 reports included investments which addressed security, resilience, and cybersecurity. Going forward, DHS security grant content and future DHS IPT R&D reports will be reviewed annually through the TSS RDWG and DHS's sub-IPTs for accuracy in enveloping evolving security and resilience considerations.

All critical infrastructure sectors are vulnerable to evolving cyber threats. A mandate from Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, and growing critical infrastructure cybersecurity risks led to the publication of the National Institute of Standards and Technology (NIST) Cybersecurity Framework in February 2014. The NIST Cybersecurity Framework provides a framework for approaching cybersecurity and managing cyber risks by assembling standards, guidelines, and practices that work effectively, applying principles and best practices to improve security and resilience.

The Sector continued to address a need to improve cybersecurity processes through increasing its communication of best practices, existing resources, and private sector solutions. The Sector shared this information via cybersecurity exercises and cybersecurity education materials, including a weekly newsletter from the TSS Cybersecurity Working Group, and cybersecurity alerts. TSA's Office of Intelligence and Analysis (I&A) distributed messages to the private sector using weekly incident information bulletins from the Surface Public Transportation Information Sharing and Analysis Center (ISAC).

Co-SSAs implemented a robust process to promote and track the adoption and implementation of the NIST Cybersecurity Framework including cyber workshops, Sector-specific resources, and the introduction of the DHS Critical Infrastructure Cyber Community (C³) Voluntary Program to Sector partners. In June 2015, the Sector published the Transportation System Sector

Cybersecurity Framework Implementation Guidance to provide guidance, resource direction, and a directory of options to assist Sector partners in adopting the NIST Cybersecurity Framework. The C³ Voluntary Program provided assistance to support stakeholders for adopting the NIST Framework, understanding cyber risk management efforts, providing outreach and communication resources, and receiving public and private sector feedback. TSA's Policy, Plans and Engagement (PPE) worked in coordination with its Coordination and Analysis and Aviation Divisions, TSS co-SSAs, TSA's Information Technology, Intelligence and Analysis office, and the Surface Transportation Security Inspector Program. TSA PPE also worked with the DHS Office of Cybersecurity and Communications within the National Protection and Programs Directorate to generate cybersecurity awareness and outreach across stakeholders.

Among its initiatives, TSA developed, promoted, and conducted a series of four regional surface transportation-focused half day cybersecurity workshops in FY 2017 in partnership with the DHS Office of Cybersecurity & Communications. The workshops were co-hosted by a local surface transportation owner/operator and in conjunction with the local TSA Surface Inspector office. The workshops provided an awareness of existing U.S. Government cybersecurity support programs and the many "no-cost" cybersecurity resources that are available to owners and operators of critical infrastructure. Additionally, the facilitated discussion component served as an opportunity for participants to both discuss industry's cybersecurity challenges and share best practices. TSA also published and disseminated the Surface Transportation Cybersecurity Resource Toolkit for Small & Midsize Business (SMB) to Sector stakeholders, which provides guidance on how to incorporate cyber risk into an organization's existing risk management and governance process.

In the aviation sub-sector, the Aviation Government Coordinating Council (AGCC) established a cybersecurity working group in 2017. As of November 2018, that working group is being migrated to the Critical Infrastructure Partnership Advisory Council construct under the joint auspices of the AGCC and the Aviation Sector Coordinating Council (ASCC).

Next Steps

- Eliminate obsolete Sector activities and revise activities to reflect new Sector priorities.
- Promote standardized security and resilience-focused language for consideration in new grants.
- Continue TSS RDWG collaboration to assess R&D prioritization. Identify and advocate Sector cyber gaps for R&D prioritization.
- Complete the initial identification and prioritization of cyber-dependent critical infrastructure and systems across the Sector.
- Continue to support the Sector's adoption of current and future NIST Cybersecurity Framework versions. Identify and create processes to manage cyber risks occurring through Sector dependencies and interdependencies.
- Charter the AGCC-ASCC cybersecurity working group.

Goal 2 – “Employ the Transportation Systems Sector response, recovery, and coordination capabilities to support whole community resilience.”

GOAL 2		
Average Score: 4.0		
Activity		Score
 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.		
 Enhance critical infrastructure preparedness for all-hazards (all modes).		
 Collaboratively identify and assess critical transportation infrastructure to manage risks and improve community resilience.		
 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.		
 Improve relationships among Sector stakeholders at the transportation industry CEO, senior government, and State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC) levels.		
 Develop exercise injects to understand priorities for improving transportation resilience for highest threat scenarios.		
 Support activities (exercises and operations) that build coordination and interoperability during responses and recovery operations.		

Overview

Sector response, recovery, and coordination capabilities are tested during real world incidents, but opportunities to enhance the employment of these capabilities can be sought out long before an incident occurs. Through Goal 2 activities, the Sector sought to increase whole community resilience using its response coordination capabilities and prompting a proactive focus on resilience across stakeholders. Goal 2 activities reframed grant requirements to include: (1) security and resilience planning as a condition of receipt, (2) engaging stakeholders in improving access to disaster sites, (3) improving stakeholder relationships, and (4) crafting exercise injects and priorities to capture transportation resilience needs and interoperability during response and recovery operations. The Sector received an average Goal 2 score of 4.0.

Highlights

The Sector solidified and enhanced public and private stakeholder relationships through the CIPAC, modal GCCs, Sector Coordinating Councils (SCCs), and SLTTGCC. Stakeholder engagement advanced situational awareness through education and the application of best practices and lessons learned related to critical infrastructure security and resilience. The Sector also assessed key elements of critical infrastructure preparedness to include developing priorities through interagency and stakeholder engagement.

Co-SSAs addressed the National Preparedness Goal five mission areas through stakeholder collaboration—prevention, protection, mitigation, response, and recovery. DOT represented the Sector through its participation in the FEMA-led Emergency Preparedness Working Group (EPWG), which promotes the National Preparedness Goal through executing preparedness programs nationally among Sector partners and transportation stakeholders. In addition, DOT participated in FEMA’s Mitigation Framework Leadership Group (MitFLG) which provides education and policy resources to government and industry related to mitigation for natural and manmade disasters. Through its MitFLG participation, DOT continues to provide leadership and direction to interagency representatives in the development of a National Mitigation Investment Strategy. DOT also participates in the Recovery Support Function Leadership Group (RSFLG), yielding greater coordination between Recovery Support Function national leads and sector partners. TSA facilitated a targeted discussion with TSA planners regarding the importance of community resilience. Through state and local partners, using modal GCCs and the SLTTGCC as a platform, the Sector garnered collective actions toward resilience efforts and prioritizing critical infrastructure.

Through the (1) National Exercise Program (NEP), (2) the Homeland Security Exercise and Evaluation Program, (3) subordinate, and concurrent exercises the Sector provided support in a controlled environment to test, validate, and improve specific plans and capabilities for responding to high threat scenarios. For example, the Sector participated in the National Level Exercise (NLE) in May 2018, examining four national-level themes: (1) Pre-Landfall Protective Actions, (2) Sustained Response in Parallel with Recovery Planning, (3) Continuity in a Natural Disaster, and (4) Power Outages and Critical Interdependencies. The Sector also supported exercise development and orchestration to build coordination and interoperability capability during response and recovery operations. The Sector contributed to FEMA through crafting real

world after-action efforts learned from the 2017 hurricane season. Lessons learned from the after-action efforts also assisted in designing NLE 2018.

Between January and August 2018, there were over 20 TSA Intermodal Security Training and Exercise Program (I-STEP) exercises. I-STEP assists transportation partners with building and sustaining security preparedness through use of an online exercise tool and guiding public and private partners through the exercise planning process. Co-SSAs are now vetting I-STEP for new opportunities to improve communication and capture best practices for future transportation-related exercises and assessments.

During response and recovery phases of incidents, it can be challenging to streamline access and re-entry and enable safe, secure, and effective access coordination between emergency managers, law enforcement, first responders, and the public and private sector organizations. In 2016, DHS established the Crisis Event Response and Recovery Access (CERRA) Working Group to improve access to national disaster sites for response and recovery teams that resulted in the 2018 publication of a framework and applicable milestones for improving disaster site access and coordination across multi-level stakeholders. The CERRA Framework focuses on supporting state, local, and regional efforts to enable the successful transit and access of critical response and recovery resources before, during, and after emergencies. The Framework builds upon prior and existing efforts by the Emergency Services Sector Coordinating Council (ESSCC) and multiple State and local crisis access and re-entry programs to cooperatively define a common approach based on best practices to enhance communities' preparation, response, recovery, and resilience efforts during incident management operations. Although a great starting point, the CERRA Framework is voluntary guidance. There is still work required to promote and integrate common practices for CERRA into SLTT government's emergency preparedness planning.

Next Steps

- Eliminate obsolete Sector activities and revise activities to reflect new Sector priorities.
- Better leverage private sector engagement into Sector response, recovery, and coordination capabilities, to include exercise development.
- Address Sector and cross-sector dependencies and interdependencies in the Sector's exercises portfolio and expand exercise participation to include international partners.
- Determine private sector priorities and needs for response, recovery, and coordination initiatives.
- Identify and implement the most effective coordination and communication processes to improve private sector engagement during incident response and recovery efforts.

Goal 3 – “Implement processes for effective collaboration to share mission essential information across sectors, jurisdictions, and disciplines and between public and private stakeholders.”

GOAL 3		
Average Score: 3.6		
Activity		Score
12	Improve collaborative processes for effectively defining and improving security and resilience intelligence requirements.	5 
13	Create a collaborative process to identify information sharing processes between subsector GCCs and SCCs.	4
14	Strengthen cybersecurity information sharing processes between subsector GCCs and SCCs.	3
15	Work with DHS to adjust the focus of Regional Resilience Assessment Program (RRAP) to capitalize on relationship building potential.	4
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.	4
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.	3
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.	3
19	Update and share recommended practices and lessons-learned from assessments and exercises.	3

Overview

The Sector shared mission essential information across sectors, jurisdictions, and disciplines, as well as between public and private stakeholders by: (1) identifying capability gaps, (2) disseminating and receiving pertinent information, (3) strengthening coordination of intelligence and cybersecurity information, (4) capitalizing on relationships to address security and resilience projects and operations, and (5) sharing recommended practices and lessons learned from assessments and exercises. The Sector earned an average score of 3.75 for Goal 3.

Highlights

Effective collaboration is vital when addressing a range of infrastructure resilience issues that could have regional and national consequences. Co-SSAs supported the DHS Regional Resilience Assessment Program (RRAP), a cooperative assessment program for specific critical infrastructure within a designated geographic area. The goal of RRAP is to generate a greater understanding among the public and private sectors to improve the resilience of a region's critical infrastructure by: (1) resolving infrastructure security and resilience knowledge gaps, (2) informing risk management decisions, (3) identifying opportunities and strategies to enhance infrastructure resilience, and (4) improving critical partnerships among the public and private sectors. Stakeholders assessed RRAP national projects to determine how the Sector could provide input on resilience projects valuable to their mutual interests. DOT's Regional Transportation Representatives (RETREP) were involved in national projects through RRAP. RETREP supports the National Response Program dedicated to coordinating DOT's preparedness, response, and recovery activities in all-hazards incidents. RETREPs handle day-to-day program issues and coordinate disaster and special events planning efforts between DOT and Federal, State, local, Tribal and Territorial, and private sector emergency planners. During incident and event responses, RETREPs lead transportation operations in FEMA's various operation centers in headquarters and affected regions. The RRAP leveraged RETREPs for insight into existing regional transportation recovery plans, the evolution of operations described in regional transportation recovery plans, and alignment of federal capabilities for future support.

Real world experiences during the 2017 and 2018 hurricane seasons highlighted the importance of effective coordination between the public and private sectors on response activities and demonstrated interdependencies across critical infrastructure sectors. In 2017, DOT's RETREPs served as active partners in the AMSCs in over 40 USCG sectors nationwide. AMSCs are composed of stakeholders who have interest in the security of the area and experience in maritime or port security operations (Federal, State, Local, Tribal and Territorial, law enforcement, emergency response, maritime industry, etc.). AMSCs are responsible for: (1) identifying critical port infrastructure and operations, (2) identifying risks, (3) determining mitigation strategies and implementation methods, (4) developing and describing the process to continually evaluate overall port security, and (5) providing advice to assist in developing an Area Maritime Security Plan.

Sector representatives engaged daily with various elements to conduct response efforts including: daily coordination between FEMA, Emergency Support Function (ESF)-1, and the interagency (via the National Business Emergency Operations Center), providing real-time updates and situational awareness. Improvements to coordination between the public and private sector during response activities are ongoing.

Next Steps

- Eliminate obsolete Sector activities and revise activities to reflect new Sector priorities.
- Identify information sharing gaps between the public sector and private sector.
- Better support the private sector through identifying needs and available resources related to training exercises for enhancing critical infrastructure and resilience.
- Assess shared interest areas with private sector stakeholder organizations to better coordinate processes and to promote information sharing.
- Map the Sector's ecosystem for interdependencies and identify shared vulnerabilities.
- Find opportunities to engage with international partners best practices for information sharing related to transportation systems and assets.

Goal 4 – “Enhance the all-hazards preparedness and resilience of the global transportation system to safeguard U.S. national interests.”

GOAL 4

Average Score: 3.2

Activity	Score
<p>20 Identify, assess, and prioritize efforts to manage supply chain risk using layered defenses in a changing security and operational environment.</p>	
<p>21 Periodically assess supply chain security risks for all ports that ship cargo to the United States under the Cargo Security Initiative.</p>	
<p>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.</p>	
<p>23 Identify and address critical infrastructure supply chain cross-sector dependencies.</p>	
<p>24 Identify and use lessons learned from supply chain disruption events to inform policies and programs that enhance our Nation’s preparedness.</p>	
<p>25 Finalize standards for air cargo advance information requirements.</p>	



Identify, assess, and prioritize efforts to manage supply chain risk using layered defenses in a changing security and operational environment.



Periodically assess supply chain security risks for all ports that ship cargo to the United States under the Cargo Security Initiative.



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.



Identify and address critical infrastructure supply chain cross-sector dependencies.



Identify and use lessons learned from supply chain disruption events to inform policies and programs that enhance our Nation’s preparedness.



Finalize standards for air cargo advance information requirements.



Overview

During an all-hazards incident, the global supply chain is vulnerable to disruption that could significantly impact public health, welfare, and economic activity. The global transportation system is an integral part of the global supply chain. To support a resilient global supply chain, the Sector identified Goal 4 activities that focused on enhancing all-hazards preparedness and resilience of the global transportation system to safeguard the global supply chain, described as a national priority in the National Security Strategy. Activities included: (1) actions to identify, assess, and prioritize risks to the supply chain; (2) improve supply chain intelligence and operational (e.g., cargo movement) information sharing; and (3) detect Sector-linked supply chain cross-sector dependencies.

The USCG leads multiple supply chain risk management efforts via its ongoing cargo security efforts. It also employs an aggressive threat identification and collection process and works with law enforcement and intelligence agencies to enhance operational and information sharing channels. Overall, the Sector earned a score of 3.2 for Goal 4. This means that only a portion of proposed expectations of this goal and subordinate activities were met. Additional opportunities exist for Sector work expansion with regards to supply chain-related efforts.

Highlights

The USCG first reviewed the Global Supply Chain Security Strategy and Implementation Plan for Sector equities. The Sector assessed transportation equities and connected security measures in the global supply chain to support the following Strategy goals: 1) Promote the efficient and secure movement of goods; and 2) Foster a resilient supply chain.

As a function of ongoing cargo security efforts, the USCG and CBP employ an aggressive threat identification and collection process by working with other law enforcement and intelligence agencies. Coupling threat identification with advance notices of arrival, Coast Guard Captains of the Port determine the risk to the vessels' transit, transfer, and cargo storage along the waterfront. The USCG also develops and implements plans that reduce the vulnerability to an attack. This may involve armed USCG escorts of dangerous cargo vessels through higher risk areas—such as high population concentration or critical infrastructure locations. Ports, vessels, and facilities to which vessels moor and transfer continue to operate under USCG-approved security plans that outline stakeholders' methods for mitigating vulnerability to attacks and follow-on consequences. The USCG's routine inspections of vessels and facilities ensure stakeholders are meeting their responsibilities under Public Law 107-295, *Maritime Transportation Security Act (MTSA)*. DHS enforces the Transportation Worker Identification Credential (TWIC) program to reduce the vulnerability to insider threats. TWIC established a foundation to identify, assess, and prioritize Sector risks to the supply chain. However, a gap existed in supply chain intelligence between Customs and Border Patrol (CBP) and the Office of Naval Intelligence that USCG identified and worked to rectify.

The Sector's aviation industry plays a large role in managing risks to the global supply chain. In June 2018, the Air Cargo Advance Screening (ACAS) program went into effect, requiring advanced submission to CBP of air cargo information on shipments arriving in the United States from a foreign location. ACAS leverages DHS threat information, and other data, to employ a risk-based approach to improving air cargo security through targeted vetting. At the National Targeting Center, CBP and TSA jointly select and mitigate high-risk cargo before it is loaded aboard aircraft headed to the United States. ACAS was developed through a 2010 pilot program that progressed through scenario-based tests and analyses until the program was validated in December 2017. The Sector is confident that ACAS will continue to help secure the nation's airports and facilities and support a resilient global supply chain.

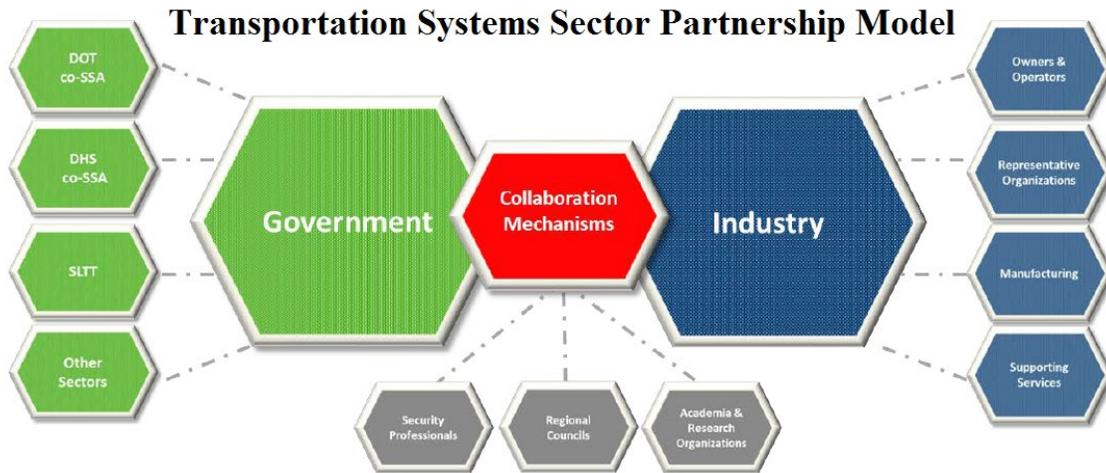
Beyond intelligence and security gaps, co-SSAs looked to further define its supply chain cross-sector dependencies that could generate vulnerabilities in the global transportation system and to the global supply chain. The Sector conducted a survey with all 16 critical infrastructure sectors regarding perceived sector-dependency on the transportation system for restoring essential community supply chains during post-incident response for a "worst case" disaster scenario (11 sectors responded). The results of the survey revealed existing cross-sector dependencies between each of the critical infrastructure sectors and each mode of transportation. Additionally, the survey results highlighted a deficit across sectors in capturing supply chain dependencies related to transportation needs.

Next Steps

- Eliminate obsolete Sector activities and revise activities to reflect new Sector priorities.
- Capture what the private sector perceives as Sector threats to the national and global supply chains, the national transportation system, and contributing private sector stakeholders direct assets.
- Identify support and resources that could better serve the Sector in supply chain risk management efforts.
- Evaluate if supply chain influence should be considered in critical infrastructure prioritization.
- Create mutual support practices and opportunities across the Sector for information sharing related to the movement of goods through the global supply chain using transportation system assets.
- Integrate supply chain resilience concepts and objectives into exercises within the Sector.
- Evaluate multimodal supply chain dependencies across the Sector.
- Collect and share Sector best practices in supply chain risk management.

Private Sector Pacesetters

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. The diagram below is the Transportation Systems Sector Partnership Model which illustrates the network used for collaboration across Sector stakeholders.



Throughout this network within the Sector, private stakeholders have carried out numerous initiatives that serve as examples for effective approaches to bolster critical infrastructure security and resilience. The following Suffolk County “Pacesetter” example demonstrates a critical infrastructure security and resilience initiative carried out by private sector stakeholders within the Sector. Private companies own and operate much of the Sector’s critical infrastructure and they have primary responsibility for the security and resilience of their operations. Making a stronger effort at recognizing and sharing private sector contributions to improving transportation systems critical infrastructure security and resilience remains vital to Sector growth.

School Bus Operators, School Districts & Emergency Responders Partner with TSA to Enhance Bus Threat Response

Suffolk County, New York (NY)

On May 23, 2018, 13 school districts in Suffolk County, NY joined local emergency responders, including Suffolk County Police, Suffolk County Office of Emergency Management, Bay Shore Fire Department, and the New York School Bus Contractor's Association in a customized TSA tabletop training exercise to improve operational coordination between school bus operators and other agencies in emergency situations. School district participants and observers included security and transportation officials, as well as senior administrators.

TSA and Suffolk Transportation Service (STS) collaborated to design the customized transportation security exercise, focused on enhancing security capabilities, to include intelligence and information sharing, planning, and physical protective measures. Transportation Security Inspectors assisted STS by using TSA's online Exercise Information System (EXIS) to design, document, and evaluate prevention, protection, and response capabilities among local stakeholders in the event of an attack on a school bus. EXIS guides government and industry users through the exercise planning process and provides resources to exercises for all transportation modes to collaborate, share information, and learn critical lessons to strengthen industry security plans, emergency procedures, and sharpen skills in incident management. The EXIS tabletop exercise enabled STS to successfully test planning efforts to protect against and coordinate a response to progressive bus attack scenarios.



“Our top priority as a school bus operator is student safety. Suffolk Transportation Service, Inc. is pleased to be selected to spearhead this training program in Suffolk County, which helped all participants enhance their coordination with other agencies to keep students safe.”

~ John Corrado, President of STS



Appendix A: Acronyms and References List

Acronym List

ACAS	Air Cargo Advance Screening
AGCC	Aviation Government Coordinating Council
ASCC	Aviation Sector Coordinating Council
AMSC	Area Maritime Security Committee
CBP	U.S. Customs and Border Protection
CERRA	Crisis Event Response and Recovery Access
CIPAC	Critical Infrastructure Partnership Advisory Council
DHS	U.S. Department of Homeland Security
DHS/IP	Office of Infrastructure Protection
DOT	U.S. Department of Transportation
EPWG	Emergency Preparedness Working Group
ESF	Emergency Support Function
EXIS	Exercise Information System
FEMA	Federal Emergency Management Agency
GCC	Government Coordinating Council
IS&S	Information Sharing and Safeguarding
ISAC	Information Sharing and Analysis Center
I-STEP	Intermodal Security Training and Exercise Program
ITDS	International Trade Data System
KIQ	Key Intelligence Questions
MitFLG	Mitigation Federal Leadership Group
MOU	Memorandum of Understanding
MTSA	Maritime Transportation Security Act
MTSA	Maritime Transportation System
NCIPP	National Critical Infrastructure Prioritization Program

NEP	National Exercise Program
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
NLE	National Level Exercise
NRF	National Response Framework
NVIC	Navigation and Vessel Inspection Circular
PIR	Priority Intelligence Requirements
PPD	Presidential Policy Directive
R&D	Research and Development
RDWG	Research and Development Working Group
RETREP	Regional Transportation Representative
RRAP	Regional Resilience Assessment Program
RSFLG	Recovery Support Function Leadership Group
S&T	Science and Technology
SCC	Sector Coordinating Council
SLTT	State, Local, Tribal, and Territorial
SLTTGCC	State, Local, Tribal, and Territorial Government Coordinating Council
SOP	Standard Operating Procedures
SSA	Sector-Specific Agency
TS SSP	Transportation Systems Sector-Specific Plan
TSA	Transportation Security Administration
TWIC	Transportation Worker Identification Credential
USCG	United States Coast Guard

References

2017 National Preparedness Report, August 28, 2017

Crisis Event Response and Recovery Access (CERRA) Framework: An Emergency Preparedness Access Implementation and Best Practice Guide, March 13, 2018

Government Accountability Office (GAO) Report to the Committee on Homeland Security, House of Representatives 16-79, Critical Infrastructure Protection, Sector-Specific Agencies Need to Better Measure Cybersecurity Progress, November 2016

Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, February 12, 2013

National Disaster Recovery Framework, Second Edition, June 2016

National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience, June 6, 2013

National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, April 16, 2018

National Preparedness Goal, Second Edition, September 2015

National Response Framework, Third Edition, June 2016

National Security Strategy of the United States of America, December 2017

National Strategy for Global Supply Chain Security Implementation Update, January 2013

National Strategy for Global Supply Chain Security, January 2012

Presidential Policy Directive (PPD)-21, Critical Infrastructure Security and Resilience, February 12, 2013

Presidential Policy Directive (PPD)-8, National Preparedness, March 30, 2011

Public Law 107-71, Aviation and Transportation Act, November 19, 2001

Public Law 107-295, Maritime Transportation Security Act of 2002, November 25, 2002

Transportation Systems Sector-Specific Plan, 2015

TSA Program Prepares School Districts, Bus Operators and Emergency Responders for Threats to Buses, *The Yellow Bus Newsletter*, Latham, NY, June 2018, p. 20

Appendix B: Transportation Systems Sector Activity Summary Reports

ACTIVITY #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.

ACTIVITY SCORE

4 *Substantial Activity Achievement*

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however, all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

The Sector focused its attention on contributing to the development of the National CISR R&D Plan, required by PPD-21, and reviewing DHS transportation-related security grants.

HIGHLIGHTS

- The Sector contributed to the development of the national CISR R&D Plan, published in November 2015, and its Implementation Roadmap. The Implementation Roadmap identified R&D priorities and presented concrete activities Executive departments and agencies will conduct over a ten-year span.
- DHS reviewed existing transportation-related DHS grants for inclusion of security and resilience prioritization and receipt requirements.
- DHS transit and port security grant programs, provisioned through FEMA, were revised to better capture security and resilience priorities and grant requirements conditional to applicants being awarded a grant.

NEXT STEPS

- Continue promotion of standardized security and resilience-focused language for consideration in new DHS grants.
- Work with SCCs, CIPAC, and other partnerships and established mechanisms to announce, coordinate and accomplish the Sector-related activities set out in the CISR R&D Plan Implementation Roadmap.

ACTIVITY #2

Jointly determine security, resilience, and cybersecurity capability gaps through the Sector's collaborative R&D prioritization process.

ACTIVITY SCORE

5

Activity Complete



The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

This activity supports the Sector in effectively identifying and mitigating security, resilience and cybersecurity capability gaps through various Sector-related R&D prioritization processes. DHS's IPT R&D Report served as a vehicle to rectify identified Sector capability gaps in technology.

HIGHLIGHTS

- DHS S&T gathered public and private surface transportation stakeholder input for R&D prioritization through the CIPAC TSS RDWG. DOT contributed through the TSS RDWG, also serving as a member to DHS's "Enhance Security" sub-IPT, chaired by TSA. DHS S&T published IPT R&D reports for FY 16 and FY 17.
 - On August 17, 2016, the TSS RDWG began R&D prioritization consideration using R&D planning guidance outlined in the TS SSP. The TSS RDWG reviewed existing Sector R&D projects and previously unfunded project requests.
 - On September 28, 2016, the TSS RDWG captured R&D gaps that should be addressed in the IPT R&D FY 16 Report.
 - On October 25, 2016, the TSS RDWG approved proposed FY 17 capability gaps.
 - In 2017, the TSS RDWG repeated this review process to contribute to the IPT R&D FY 17 Report.

NEXT STEPS

- Continue to update R&D prioritization for Sector initiatives through TSS RDWG and DHS sub-IPT engagement.

ACTIVITY #3

Identify and prioritize cyber-dependent critical infrastructure and systems.

ACTIVITY SCORE

1 *No Activity Progress*

The Sector has not initiated work toward the requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported the achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity supports the Sector in identifying and prioritizing cyber-dependent critical infrastructure and systems for all modes. The Sector conducts a bi-annual or quadrennial study to update its priorities.

HIGHLIGHTS

- At the cyber workshop with the TSS Cyber Working Group, held on November 1, 2017, co-SSAs requested private sector support for identifying critical infrastructure. The TSS Cyber Working Group has not convened on a regular basis since this need was identified and as a result progress for prioritizing cyber dependent infrastructure and systems stalled.
- Co-SSAs plan to reconvene the TSS Cyber Working Group in the near future. The objective of reconvening will be to prioritize cyber-dependent infrastructure and systems, with a focus on current, new, and future programs, by working through the following steps with industry support:
 - Identify cyber-dependent critical infrastructure with modal partners.
 - Establish initial cyber-dependent critical priorities.
 - DHS's Office of Cyber and Infrastructure Analysis will conduct a systems-based analysis and determine gaps.
 - Determine final priorities and report development.
 - Disseminate a report and modify existing practices.

NEXT STEPS

- Reconvene the TSS Cyber Working Group.
- Complete initial identification and prioritization of cyber-dependent critical infrastructure and systems across the Sector.
- Maintain prioritized list of cyber-dependent critical infrastructure and systems, revise as needed.

ACTIVITY #4

Encourage adoption of the NIST Cybersecurity Framework.

ACTIVITY SCORE

5 *Activity Complete* 

The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

This activity involved two major components: 1) encourage the adoption of the NIST Cybersecurity Framework, and 2) measure the cybersecurity posture of owners and operators within the Sector.

HIGHLIGHTS

- The Sector implemented a robust process to promote and track the adoption and implementation of the NIST Cybersecurity Framework, using its regional cyber workshops and the DHS Critical Infrastructure Cyber Community Voluntary Program.
- In June 2015, the Sector published the Transportation Systems Sector Cybersecurity Framework Implementation Guidance to provide guidance, resource direction and a directory of options to assist in adopting the NIST Cybersecurity Framework.
- DHS carried out C³ Voluntary Program outreach to include providing a messaging kit.
- The DHS C³ Voluntary Program focused on:
 - Assisted stakeholders with understanding use of the Framework and other cyber risk management efforts, and supported development of sector-specific guidance for Framework implementation.
 - Served as a point-of-contact and customer relationship manager to assist organizations with Framework use, and guided interested organizations and sectors to DHS and other public and private resources to support the use of the Framework.
 - Encouraged feedback from stakeholder organizations.
- In April 2018, Version 1.1 of the NIST Cybersecurity Framework was published. DHS and DOT participated updating the Framework by providing Sector- and agency-specific input. DHS and DOT continue to promote Sector-wide adoption of the Framework.

NEXT STEPS

- Collect and advocate Sector cyber needs and challenges for consideration for future versions of the NIST Cybersecurity Framework.
- Continue to support the Sector in adopting current and future NIST Cybersecurity Framework versions.

ACTIVITY #5

Develop incentives to increase cybersecurity.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported the achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

Develop incentives to increase cybersecurity by: (1) facilitating employee training opportunities, (2) recognizing industry achievements in cybersecurity, (3) certifying and confirming security measures as a condition for grant awards, and (4) promoting participation across all modes in DHS voluntary initiatives.

HIGHLIGHTS

- DHS held a Cyber Workshop on November 1, 2017 with TSS CWG membership.
- DHS's Office of Cybersecurity & Communications, TSA's Surface Inspector Office, and local surface transportation owners and operators hosted four regional transportation-focused cybersecurity workshops in 2017. The workshops provided information on existing government cybersecurity support programs and resources, and provided an opportunity to facilitate public and private sector discussion regarding Sector-related cybersecurity challenges and best practices.
- Co-SSAs also participated in the American Public Transportation Association Enterprise Cybersecurity Working Group, the Control and Communications Systems Working Group, and various national and regional cybersecurity panels and conferences.
- The USCG has issued Navigation and Vessel Inspection Circular (NVIC) 04-18, "Guidelines For Drafting The Marine Transportation System (MTS) Recovery Plan," to provide guidance to field commanders, Marine Transportation Recovery personnel and the maritime community to develop and maintain the MTS Recovery Plan. This NVIC provides a common template for the development of MTS Recovery Plans to address all hazards, MTS recovery processes and procedures while promoting unity of effort among all stakeholders with MTS recovery interests within each Captain of the Port zone.

NEXT STEPS

- Coordinate with public and private sector partners to promote cybersecurity awareness, education, and training, as Sector cybersecurity challenges and best practices evolve.

ACTIVITY #6

Enhance critical transportation infrastructure preparedness for all-hazards.

ACTIVITY SCORE

4 *Substantial Activity Achievement*

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however, all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity encompasses a broad range of preparedness activities to support resilience across all modes targeted at assessing key elements of critical infrastructure preparedness and exploring and promoting enhancement of critical infrastructure preparedness. The implementation approach focused on jointly developing priorities through interagency and stakeholder engagement and advancing situational awareness, training, education, and application of best practices.

HIGHLIGHTS

- DOT continued broad participation in PPD-8 implementation efforts, aimed at strengthening the security and resilience of the United States through systematic preparation for threats which pose the greatest risk to the security of the Nation.
 - DOT participated in the FEMA-led EPWG and its annual program of coordinated all-hazards preparedness activities focused on natural disasters. Participation enabled DOT to promote the National Preparedness Goal among Sector partners nationwide.
 - DOT participated in FEMA’s MitFLG, including participation in the development of the MitFLG work plan and promotion of “Mitigation Saves” materials supported risk-informed decision making regarding hazard identification, assessment, and best practices in reducing and preventing damage.
 - DOT participated in the development of the MitFLG’s National Mitigation Investment Strategy, developed due to a recommendation from the GAO report on Hurricane Sandy.
 - DOT participated in the RSFLG, RSFLG Action Officer meetings and work plan implementation (throughout 2016-17), yielding greater coordination between Recovery Support Function national leads and Sector partners.
 - DOT participated in the FEMA Risk Management Directorate’s “100 Resilient Cities” program, exploring and promoting resilience efforts in major urban areas. (February 2018).
- The Sector participated in the DHS 2018 Critical Infrastructure Summit which advanced education and situational awareness through sharing up-to-date information on critical infrastructure programs, technology, efforts and challenges across all sectors. Sector representatives participated in various sessions covering topics such as cybersecurity, critical infrastructure and the 2017 hurricane season. The Sector also featured a display booth to inform other sectors on the transportation modes as well as the overall role of the Transportation Systems Sector (March 2018).

NEXT STEPS

- Capture Sector input for contribution to existing and future National Security Council directed preparedness policy development initiatives.
- Determine private sector evolving priorities and needed support for preparedness initiatives.

ACTIVITY #7

Collaboratively identify and assess critical infrastructure to improve community resilience.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity encompasses a range of preparedness activities to support whole community resilience across all modes within the broad scope of NIPP and TS SSP implementation via promotion of public-private sector coordination, to include interactions with the SLTTGCC and other stakeholder organizations.

HIGHLIGHTS

- The Sector participated in a variety of broad NIPP and Sector implementation efforts.
 - In 2017, TSA staff facilitated a targeted discussion with TSA planners about the importance of community resilience.
 - Co-SSAs continuously engaged with state and local partners through the SLTTGCC to foster coordination and promote “whole community” resilience across the Sector. Interactions demonstrated that states and localities have a unique view of what assets should be identified as critical and view respective owned assets and infrastructure from a system perspective rather than a larger community or national perspective.
- Enhanced engagement with Modal GCCs through the quarterly Modal GCC meetings.
- Co-SSAs provided input to the National Preparedness Report and National Annual Report facilitating a framework for collective action for achieving a more secure and resilient nation.

NEXT STEPS

- Continue collaboration with the SLTTGCC to capture their views on critical infrastructure in national efforts.
- Continue engagement with Modal GCC Co-Chairs.
- Leverage the annual National Critical Infrastructure Prioritization Program (NCIPP) review cycle to facilitate sector partner engagement in the NCIPP annual update and identify opportunities to promote community resilience.
- Participate in cross-sector 2018 Policy Leadership Working Group co-chaired by the IT GCC- looking at cybersecurity regulations impacting the IT Sector, as well as exploring the nation’s “collective defense” against cyber-attacks from nation states and other sophisticated actors.
- Participate in 2018 and 2019 NIPP and SSP refresh activities.

ACTIVITY #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.

ACTIVITY SCORE

5

Activity Complete



The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

This activity served as an introductory step to connect stakeholders through efforts to establish jointly developed priorities, planning efforts, building partnerships, enabling risk-informed decision making and situational awareness, identifying and assessing critical infrastructure and resilience, and adapting to new developments. A sector-level forum was established to improve access to national disaster sites for response and recovery teams. This resulted in supporting a framework and applicable milestones that illustrated the determined courses of action for access improvement. Although a great starting point, the framework developed is voluntary guidance. There is still work required to promote and integrate common practices for CERRA into SLTT government's emergency preparedness planning.

HIGHLIGHTS

- Sector efforts to create a forum to address the issue of disaster site credentialing began with internal DOT outreach in July 2016, with DOT convening an internal meeting to request input from its Operating Administrations.
- In November 2016, DHS convened a cross-sector CERRA working group with the goal of creating a framework for a common access and re-entry approach and enabling “*safe, secure, and effective access coordination between emergency managers, law enforcement, first responders, including public, private, and volunteer/non-government organization sectors.*” The CERRA working group continues to meet on a quarterly basis.
- Discussion among working group members clarified that access and re-entry considerations are a state-by-state issue and thus adopted the framework approach to provide voluntary guidance.
- The working group continued framework development with several rounds of review:
 - Internal drafts among working group members for proof-of-concept and critical issues.
 - An initial draft for stakeholder review (May 2017); wider circulation by Office of Infrastructure Protection (DHS/IP) via the Sector Partnership distribution list (June 2017).
 - Submission to DHS/IP leadership for final review (Fall 2017) led to a clarification in the description of access levels (Appendix B, the recommended checklist) along with some language changes.
- The framework was approved for distribution on March 13, 2018.

NEXT STEPS

- In 2018, the CERRA working group will participate in a nationwide outreach strategy with public and private stakeholders and will share promotional materials under development (e.g. fact sheet, newsletter article, introductory video).
- The Sector should consider crafting Sector-specific guidance related to improving response and recovery team access to national disaster sites.

ACTIVITY #9

Improve relationships among Sector stakeholders at the transportation industry Chief Executive Officer, senior government, and SLTTGCC levels: 1) Facilitate Sector partnership through Sector and modal GCCs and SCCs, and 2) Participate in senior-level CIPAC councils.

ACTIVITY SCORE

5

Activity Complete



The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

The Sector focused on building relevant networks for critical infrastructure security and resilience priorities to foster efficient information exchange.

HIGHLIGHTS

- Co-SSAs participated in all CIPAC-related Federal Senior Leadership and Joint Cross Sector Council meetings held since publication of the TS SSP.
- In November 2017, the TSA Administrator held a public meeting of senior government and transportation industry personnel to discuss information required to develop a transportation strategic agenda.
- Through various Federal Advisory Councils, co-SSAs met regularly with senior industry officials to discuss Sector-related topics of interest, such as (1) aviation security, (2) aviation consumer protection, (3) accessible air transportation, (4) automation in transportation, (5) the future of aviation, (6) motor carrier safety, (7) travel and tourism infrastructure, (8) transit advisory safety, (9) chemical transportation, (10) rail energy transportation, and (11) towing safety.

NEXT STEPS

- The Sector management team will continue to meet with CIPAC-related councils and federal advisory committees.
- The Sector management team should encourage expanded and stronger membership participation in the modal GCCs and SCCs to provide better representation of transportation issues.

ACTIVITY #10

Develop exercise injects to understand priorities for improving transportation resilience for highest threat scenarios.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

Activities 10 and 11 identify the need for Sector stakeholders to participate in exercises and operations that increase coordination and interoperability within the whole of community with the goal of increasing resilience in the Sector. Through the NEP, the Homeland Security Exercise and Evaluation Program, and subordinate and concurrent exercises, the Sector should employ personnel and resources in a controlled environment to test, validate, and improve a specific plan or capability in pursuit of a stated objective within the homeland security enterprise and in response to the highest threat scenarios.

HIGHLIGHTS

- The Sector participated in the NLE in May 2018, examining the ability to protect against, respond to, and recover from a major Mid-Atlantic hurricane. The exercise examined four national-level themes: (1) Pre-Landfall Protective Actions; (2) Sustained Response in Parallel with Recovery Planning; (3) Continuity in a Natural Disaster; and (4) Power Outages and Critical Interdependencies.
- The Sector supported FEMA in providing real world after-action efforts from the 2017 hurricane season to incorporate lessons from Hurricanes Harvey, Irma, and Maria into the design of NLE 2018.
- The Sector continued to support TSA's I-STEP, which assists transportation partners with building and sustaining security preparedness to improve resilience.
 - The program offers an online exercise tool to guide public and private partners through the exercise planning process, available at <https://www.tsa.gov/for-industry/exercise-information-system>. The Sector also began vetting I-STEP for new opportunities to improve communication and capturing best practices for future transportation-related exercises and assessments.
 - Numerous modes are engaged in developing exercises within I-STEP with TSA's support. Between January and August 2018, over (20) I-STEP exercises were conducted, to include multimodal and interagency exercises.

NEXT STEPS

- Continue to plan, develop, conduct and evaluate single and multimodal transportation security-focused I-STEP exercises to improve transportation security preparedness.
- Continue to share best practices and lessons learned via EXIS and industry engagement managers.
- Leverage Transportation Security Inspectors to expand the breadth of I-STEP, aligning exercise planning with identified risk priorities.

ACTIVITY #11

Support activities (exercises and operations) that build coordination and interoperability during responses and recovery operations. (All modes)

ACTIVITY SCORE

4 *Substantial Activity Achievement*

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

Activities 10 and 11 identified the need for Sector stakeholders to participate in exercises and operations that increase coordination and interoperability within the whole of community with the goal of increasing resilience in the Sector. Through the NEP, the Homeland Security Exercise and Evaluation Program, and subordinate and concurrent exercises, the Sector should employ personnel and resources in a controlled environment to test, validate, and improve a specific plan or capability in pursuit of a stated objective within the homeland security enterprise and in response to the highest threat scenarios.

HIGHLIGHTS

- The Sector participated in the NLE in May 2018, examining the ability to protect against, respond to, and recover from a major Mid-Atlantic hurricane. The exercise examined four national-level themes: (1) Pre-Landfall Protective Actions; (2) Sustained Response in Parallel with Recovery Planning; (3) Continuity in a Natural Disaster; and (4) Power Outages and Critical Interdependencies.
- The Sector supported FEMA in providing real world after-action efforts from the 2017 hurricane season to incorporate lessons from Hurricanes Harvey, Irma, and Maria into the design of NLE 2018.
- The Sector continued to support TSA's I-STEP, which assists transportation partners with building and sustaining security preparedness to improve resilience.
 - The program offers an online exercise tool to guide public and private partners through the exercise planning process, available at <https://www.tsa.gov/for-industry/exercise-information-system>. The Sector also began vetting I-STEP for new opportunities to improve communication and capture best practices for future transportation-related exercises and assessments.
 - Numerous modes are engaged in developing exercises within I-STEP with TSA's support. Between January and August 2018, over 20 I-STEP exercises were conducted, to include multimodal and interagency exercise.

NEXT STEPS

- Continue to plan, develop, conduct and evaluate single and multimodal transportation security-focused I-STEP exercises to improve transportation security preparedness.
- Share best practices and lessons learned via EXIS and industry engagement managers.
- Leverage Transportation Security Inspectors to expand the breadth of I-STEP, aligning exercise planning with identified risk priorities.

ACTIVITY #12

Improve collaborative processes for effectively defining and improving security and resilience intelligence requirements.

ACTIVITY SCORE

5

Activity Complete



The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

Co-SSAs engaged with Federal, SLTT, and transportation private sector stakeholders to validate transportation intelligence requirements and share these requirements with transportation stakeholders, as authorized.

HIGHLIGHTS

- On February 3, 2017, co-SSAs discussed implementing information sharing activities with aviation and surface points-of-contact. The consensus was that another working group at the Sector-level probably would not add value. Given multiple, on-going information sharing initiatives, co-SSAs decided to distribute the activities to the modal GCCs.
- DHS initiated an effort to develop a cross-sector, five-year Information Sharing and Safeguarding (IS&S) Strategy and a separate process to identify Key Intelligence Questions (KIQs) for each sector. TSA's I&A manages and implements the TSA Administrator's Priority Intelligence Requirements (PIRs), which are developed in collaboration with industry partners to ensure that the PIRs satisfy the needs of the transportation industry and the TSA Administrator.
- The PIRs include over 50 elements of essential information that are grouped into KIQs, or analytical themes, and are used to develop TSA I&A's Program of Analysis (POA). The POA provides TSA I&A with an analytic focus and drives strategic production. End results, to include formal intelligence assessments and shorter analytical notes, are shared with the transportation industry.
- PIRs and the POA are updated every two years to generate timely and relevant analysis and assessments that drive transportation security decisions and policy efforts. These efforts strengthened the Sector's coordination of intelligence and cybersecurity information. The Sector also capitalized on existing resources and partnerships to address security and resilience initiatives.

NEXT STEPS

- Activity complete.

ACTIVITY #13

Create a collaborative process to identify information sharing capability gaps.

ACTIVITY SCORE

4 *Substantial Activity Achievement*

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however, all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity is focused on monitoring and improving the ratio of proposals submitted to DHS S&T that are selected for R&D projects.

HIGHLIGHTS

- The RDWG develops capability gaps for submission to DHS S&T and facilitates collaboration to identify information sharing capability gaps and to track and evaluate proposals submitted to DHS S&T. See Activity #2 for additional details.

NEXT STEPS

- RDWG activities are repeated annually.

ACTIVITY #14

Strengthen cybersecurity information sharing processes between subsector GCCs and SCCs.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

The Sector pursued this activity by standing up subsector information sharing and analysis bodies.

HIGHLIGHTS

- The Sector conducted two cybersecurity exercises and produced a weekly newsletter through the TSS CWG to reach across modes and encourage private sector participation.
- TSA Office of Intelligence and Analysis provided cyber threat and incident intelligence to the private sector. This support was provided through written guidance, formal briefings, and impromptu teleconferences in response to malicious cyber activities.
- The Surface and Public Transportation ISAC provided detailed weekly and incident specific information bulletins to public and private sector organizations.

NEXT STEPS

- Information sharing continues to be cited by exercise participants as the most significant gap.
- The Sector should consider conducting a gap analysis to identify areas where information sharing improvements are needed.

ACTIVITY #15

Work with DHS to adjust focus of RRAP to capitalize on relationship-building potential.

ACTIVITY SCORE

4 *Substantial Activity Achievement*

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however, all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

Sector representatives worked to: 1) explore RRAP projects nationwide, 2) assess how the Sector could provide input on resilience projects valuable to our mutual interests, and 3) use this opportunity to capitalize on relationship building potential. The implementation approach also included a review and assessment of 2017 transportation-related RRAP projects and processes.

HIGHLIGHTS

- In January 2017, DOT staff presented on DOT’s capabilities and capacity to assist with RRAP projects to raise awareness of DOT programs and activities and to increase coordination with regional partners.
 - The RRAP coordinator found the engagement beneficial through it sharing insights into: 1) what regional transportation recovery plans exist, 2) how those operations are expected to play out, and 3) what Federal capabilities exist or could be brought to bear during response and recovery operations.
 - Exploration of these public and private relationships helped the team in refining project concepts and informing future efforts.
- DOT initiated coordination with the RRAP team to identify and assess transportation-related RRAP projects and processes undertaken in recent years. Review of RRAP projects in the FY 2017 RRAP Project Matrix with a transportation nexus (6 of 15 projects) included:
 - New York City – analysis of extensive infrastructure risk data collected by New York City to provide improved understanding of dependencies and risk prioritization.
 - Port of San Diego – assessment and characterization of infrastructure to inform security and emergency management officials of its location and criticality.
 - Caribbean Supply Chain – identification and resilience assessment of supply chain components exploration of potential alternatives to support the development of response and recovery plans at all levels for supply chain disruptions.
 - Washington State Transportation System – based on observations from the 2016 “Cascadia Rising” exercise – analysis of transportation system seismic vulnerabilities and expected disruptions, response and recovery plans and capabilities, and seismic mitigation strategies.
 - Oklahoma and Arkansas River System – examination of vulnerabilities and consequences to regional infrastructure associated with their dependence on the McClellan-Kerr Arkansas River Navigation System to inform regional strategic and emergency planning efforts.

- Gulf Coast Critical Dependencies – Project identification of critical dependencies with an emphasis on the electric power of regionally significant infrastructure in Louisiana, Arkansas, Mississippi, and Texas.

NEXT STEPS

- Continue efforts to implement relationship-building processes through the RRAP for effective collaboration.
- Conduct periodic review of transportation-related RRAP projects and assessment of how they impacted regional relationships between public and private sector partners.

ACTIVITY #16

Enhance engagement with States and regions at the field level through USCG Captains of the Port, Protective Security Advisors, Federal Security Directors, DOT's Regional Transportation Representatives, and (state and local) Fusion Centers.

ACTIVITY SCORE

4 *Substantial Activity Achievement*

The Sector met the majority of requirements initially proposed in the TS SSP for the activity, however, all requirements were not met. The activity may include requirements that need to be fulfilled on a reoccurring or ongoing basis. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity promotes a variety of engagement efforts between public and private sector entities through the Sector's involvement in the security and resilience mission. Engagement efforts occur through various programs such as the USCG Captains of the Port and AMSCs, DOT's RETREPs, and other elements across the Sector. TSA is also exploring expansion of the security and resilience mission through the Federal Security Directors program.

HIGHLIGHTS

- In 2017, DOT's RETREPs served as active partners in the USCG AMSCs in over 40 USCG sectors nationwide.
- Real world experiences during the 2017 hurricane season highlighted the importance of effective coordination between the public and private sectors on response activities and demonstrated interdependencies across critical infrastructure sectors.
- Sector representatives engaged daily with various elements to conduct response efforts, including daily coordination between FEMA, ESF-1, and the interagency (via the National Business Emergency Operations Center), providing real-time updates and situational awareness. Improvements to coordination between the public and private sectors during response activities are ongoing.

NEXT STEPS

- Utilize lessons learned from the 2017 hurricane season to generate greater cross-sector coordination and public and private sector coordination. FEMA is considering adopting identified best practices by creating a new ESF explicitly focused on cross-sector planning, exercises, and mutual assistance.
- Continue implementation and outreach efforts for emerging efforts regarding response activities.
- Continue close coordination between Sector representatives, the interagency, FEMA, ESF-1, and state and local response and recovery elements to implement future security and resilience goals and activities.
- Explore private-sector stakeholder organizations to identify shared interest areas within their stated mission area.

ACTIVITY #17

DHS and DOT, through GCCs and other partnerships, engage other sectors and SLTT partners to identify interdependencies and enhance efficient use of resources.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity is focused on the Sector's priority to expand and improve partnerships to enhance resilience of communities and interdependent sectors. To facilitate identification of interdependencies and dependencies across critical infrastructure sectors, the Sector developed and initiated a survey.

HIGHLIGHTS

- On November 21, 2017, Sector representatives developed a survey to determine interdependencies and dependencies. The survey was beta-tested in the Emergency Services Sector.
- On December 17, 2017, the beta-test was distributed to all critical infrastructure sectors.
- 12 of the 16 sectors responded to the survey in February 2018.
- Sector representatives analyzed survey responses and released a report on March 18, 2018.
- Sector representatives shared the survey results and report with other critical infrastructure sectors during the April 12, 2018 National Protection and Programs Directorate, Office of Infrastructure Protection, SSA Coordination Conference Call.

NEXT STEPS

- Map the Sector's ecosystem for interdependencies and identify intertwined vulnerabilities.

ACTIVITY #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.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

The tip line will support the Sector in interagency information sharing related to all-hazard incident reporting.

HIGHLIGHTS

- In September 2016, DHS moved to establish a working group to consider the need for creating a tip line to communicate threats or suspicious incidents to appropriate authorities.
- TSA presented the activity to the Federal Senior Leadership Council on October 5, 2016.
- Vice-Chair of the Highway and Motor Carrier SCC agreed to lead the effort and presented an approach at the Joint Cross Sector Council meeting in early 2017. The USCG Military Advisor to the DHS Secretary became the project champion, completing the task to define the scope and approach for a tip line.
- Research to identify needs and challenges for supporting the tip line is ongoing.

NEXT STEPS

- Finalize tip line research.
- Launch projected for November 2019.

ACTIVITY #19

Update and share recommended practices and lessons learned from assessments and exercises.
(Industry, all modes)

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity advocates for the Sector to track and share best practices and lessons learned from assessments and exercises. The Sector's initial approach included reviewing feedback from exercise after action reports and identifying potential platforms that could offer an improved means to track and share exercise and assessment best practices.

HIGHLIGHTS

- A review and analysis of exercise after action reports and assessments was used to identify relevant lessons learned. The results were used to provide exercise injects through the NEP, including for NLE 2018.
- The Sector continued supporting TSA's I-STEP, which assists transportation partners with building and sustaining security preparedness to improve resilience. The program offers an online exercise tool to guide public and private partners through the exercise planning process, available at <https://www.tsa.gov/for-industry/exercise-information-system>. The Sector also began vetting the I-STEP for new opportunities to improve communication and capturing best practices for future transportation-related exercises and assessments.
 - In March 2018, I-STEP was used to conduct a cybersecurity workshop in Atlanta, Georgia. The workshop informed stakeholders about cybersecurity resources and programs, facilitated best practice discussions and provided multi-modal, non-technical cybersecurity training.
- Shared observations and lessons learned from the 2016 Cascadia Rising exercise led the Washington State Transportation System to uncover seismic vulnerabilities, expected disruptions, response and recovery plans and capabilities, and seismic mitigation strategies. (FY17 RRAP project).
- Sector leadership re-invigorated the TSS CWG to share recommended cybersecurity practices and challenges—the first meeting of the TSS CWG since 2014—with over 100 participants (November 2017).
- The Sector engaged in Cyberstorm VI—a NLE exploring vulnerabilities during a large-scale coordinated cyber-attack. Transportation was a main focus—examining inherent cyber vulnerabilities in automated vehicle systems, supply chain disruption, and the effectiveness of the National Cyber Incident Response Plan's enhanced coordination procedures. The exercise tested the Sector's enhanced coordination procedures, information sharing between the Sector and other agencies, and identified lessons learned and follow-up items to include forming cyber incident response procedures and communications plans. (April 2018)

NEXT STEPS

- Continue participation in exercise planning and coordination and after-action analysis.
- Update and share recommended practices from assessments and exercises.
- Implement TSS CWG priorities and work plan items.
- Assist the TSS CWG with work on contributing to a Homeland Security Information Network portal for cyber lessons learned.
- Participate in discussions through various forums regarding interagency coordination, such as the working groups and tabletop exercises.

ACTIVITY #20

Identify, assess, and prioritize efforts to manage supply chain risk using layered defenses in a changing security and operational environment.

ACTIVITY SCORE

3 *Partial Activity Achievement*

The Sector met less than the majority of requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity focuses on activities described in the National Strategy for Global Supply Chain Security and related Implementation Update. The Sector assessed transportation equities in the global supply chain and the connected security measurements to support the following Strategy goals: 1) Promote the efficient and secure movement of goods, and 2) Foster a resilient supply chain.

HIGHLIGHTS

- The Sector is identifying and assessing efforts for supply chain risk management using layered defenses. This can be seen through:
 - Supply chain-focused RRAP projects.
 - Port threat identification and cargo screening initiatives. See Activity #21 and Activity #22.

NEXT STEPS

- Explore modal interdependencies within the supply chain to further understand resilience challenges.
- Continue work on supply chain-focused RRAP projects.

ACTIVITY #21

Periodically assess supply chain security risks for all ports that ship cargo to the United States under the Cargo Security Initiative.

ACTIVITY SCORE

4 *Activity Complete*

The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

This activity focuses on activities described in the National Strategy for Global Supply Chain Security and related Implementation Update. The Sector assessed transportation equities in the global supply chain and the connected security measurements to support the following Strategy goals: 1) Promote the efficient and secure movement of goods, and 2) Foster a resilient supply chain.

HIGHLIGHTS

- As part of its on-going cargo security efforts, the USCG employs an aggressive threat identification and collection process, working with other law enforcement and intelligence agencies.
- Coupling threat identification with advance notices of arrival, USCG Captains of the Port determine the risk to the vessels' transit, transfer, and cargo storage along the waterfront.
- The USCG develops and implements plans that reduce the vulnerability to an attack. This may involve armed USCG escorts of dangerous cargo vessels through higher risk areas, such as population concentration or critical infrastructure locations.
- Ports, vessels, and facilities to which vessels moor and transfer, continue to operate under USCG-approved security plans that outline those stakeholders' methods for mitigating their vulnerability to attack and resultant consequences.
- The USCG conducted routine inspections and exercises of vessels and facilities to ensure stakeholders are meeting their responsibilities under the MTSA.
- DHS continued to enforce the TWIC program to reduce the vulnerability to insider threats.
- Under the Container Security Initiative, CBP has stationed teams of CBP Officers in foreign locations to work together with host foreign government counterparts. Their mission is to target and prescreen containers and to develop additional investigative leads related to terrorist threat cargo destined to the United States.

NEXT STEPS

- Continue assessing security risks, as appropriate.

ACTIVITY #22

Formalize information sharing arrangements between Federal agencies focused on cargo arriving and departing the United States, including law enforcement entities operating in CBP's National Targeting Center and those agencies, such as the Office of Naval Intelligence, focused on cargo moving between foreign ports.

ACTIVITY SCORE

4 *Activity Complete*

The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

This activity focuses on activities described in the National Strategy for Global Supply Chain Security and related Implementation Update. The Sector assessed transportation equities in the global supply chain and the connected security measurements to support the following Strategy goals: 1) Promote the efficient and secure movement of goods, and 2) Foster a resilient supply chain.

HIGHLIGHTS

- Aviation - See Activity 25 for information related to ACAS for inbound air cargo from foreign locations.
- Maritime – The USCG works with CBP in accordance with Standard Operating Procedures (SOPs), operational channels, and information sharing channels. For inbound and outbound cargo screening to foreign locations, the USCG:
 - Established a Memorandum of Understanding (MOU) with CBP to share Notice of Arrival and Notice of Departure information to target security efforts for vessels carrying cargo of interest.
 - Partnered with CBP and other agencies via the International Trade Data System (ITDS). The ITDS establishes a single portal system, operated by CBP, used for sharing interagency information on carriers and cargo.
 - Worked with CBP and other agencies in Multi-Agency Strike Force Operations to perform cargo checks, container inspections, personnel vetting, documentation verification, etc., at terminal gate inspection points.
 - Maintained an MOU with CBP that establishes a joint SOP for addressing potentially “high risk” crew members.
 - Established joint protocols with CBP for expeditious resumption of trade following a transportation security incident or other trade disruption.

NEXT STEPS

- Continue evaluation of information sharing arrangements and mechanisms, as requirements evolve.

ACTIVITY #23

Identify and address critical infrastructure supply chain cross-sector dependencies.

ACTIVITY SCORE

2 *Activity Work Initiated*

The Sector initiated work toward the requirements initially proposed in the TS SSP for the activity, however, no requirements have been achieved. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity focuses on activities described in the National Strategy for Global Supply Chain Security and related Implementation Update. The Sector assessed transportation equities in the global supply chain and the connected security measurements to support the following Strategy goals: 1) Promote the efficient and secure movement of goods, and 2) Foster a resilient supply chain.

HIGHLIGHTS

- On November 21, 2017, Sector representatives developed a survey to determine interdependencies and dependencies. The survey was beta-tested in the Emergency Services Sector.
- On December 17, 2017, the beta-test was distributed to all critical infrastructure sectors.
- 12 of the 16 sectors responded to the survey in February 2018.
- Sector representatives analyzed survey responses and released a report on March 18, 2018.
- Sector representatives shared the survey results and report with other critical infrastructure sectors during the April 12, 2018 National Protection and Programs Directorate, Office of Infrastructure Protection, SSA Coordination conference call.
- The results of the report demonstrated existing cross-sector dependencies between each of the critical infrastructure sectors and each mode of transportation. In addition, the report highlighted a deficit across sectors in capturing supply chain dependencies related to transportation needs.
- RRAP projects have included proposals focused on supply chain resilience, for example:
 - FY 2017 Caribbean Supply Chain – The project focused on supply chain distribution of medicine, food and fuel to and between Puerto Rico and US Virgin Islands. The project identified components of the supply chain, assessed component resilience, and identified potential alternatives to support the development of federal, territorial, and private sector response and recovery plans for supply chain disruptions.

NEXT STEPS

- Engage cross-sector and modal partners to capture supply chain dependencies related to transportation needs.
- Further promote supply chain resilience RRAP projects.

ACTIVITY #24

Identify and use lessons learned from supply chain disruption events to inform policies and programs that enhance our Nation's preparedness.

ACTIVITY SCORE

1 *No Activity Progress*

The Sector has not initiated work toward the requirements initially proposed in the TS SSP for the activity. Sector activity progress, to date, has not supported achievement of one or more priorities provided for its overarching Sector goal.

DESCRIPTION

This activity focuses on activities described in the National Strategy for Global Supply Chain Security and related Implementation Update. The Sector assessed transportation equities in the global supply chain and the connected security measurements to support the following Strategy goals: 1) Promote the efficient and secure movement of goods, and 2) Foster a resilient supply chain.

HIGHLIGHTS

- Although efforts to build best practices for supply chain risk management likely have occurred, the Sector has not yet initiated a process to collectively accomplish the scope of this activity.

NEXT STEPS

- Engage private partners through conducting a supply chain risk management best practices study.

ACTIVITY #25

Finalize standards for air cargo advance information requirements.

ACTIVITY SCORE

5

Activity Complete



The Sector met all requirements initially proposed in the TS SSP for the activity. The work completed for the activity supported achievement of one or more priorities provided for its overarching Sector goal. The activity will be assessed for alternative application to future Sector needs.

DESCRIPTION

Supporting a secure and resilient global supply chain, the ACAS requires the submission of advanced air cargo information on shipments arriving in the United States from a foreign location. ACAS will help secure the nation's airports and facilities.

HIGHLIGHTS

- ACAS was developed through a 2010 pilot program that progressed through scenario-based tests and analyses.
- In December 2017, CBP completed tests and analyses and validated information requirements.
- In June 2018, the interim final rule was published and the ACAS program went into effect. The interim final rule was open for public comments until August 2018. Carriers and other ACAS filers will work with CBP and the National Targeting Center for Cargo to achieve full operational status prior to July 2019.

NEXT STEPS

- Activity complete.

Appendix C: Glossary of Terms

Many of the definitions in this Glossary are from Federal laws, Presidential 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)

Critical Infrastructure. Systems and assets, physical or virtual, so vital to the United States that 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 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)

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)

Government Coordinating Council. The government Sector group, established to enable intergovernmental coordination, comprised of 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, cyberattacks, cyber failures and accidents, 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. 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, cyberattacks, 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. 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, 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)

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 (SSPs). 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)

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)