



TSA Cybersecurity Roadmap 2018



Transportation
Security
Administration

Administrator's Message

November 1, 2018

I am proud to present the Transportation Security Administration's Cybersecurity Roadmap. This document will guide our collective efforts to prioritize cybersecurity measures within TSA and the Transportation Systems Sector over the years ahead.

The Cybersecurity Roadmap aligns with and supports the 2018-2026 TSA Strategy. It defines clear pathways to integrate and improve the TSA's cybersecurity posture, safeguard the nation's transportation systems, and build TSA's capacity to meet the ever-changing cybersecurity environment through smart investments and collaborative partnerships.

To achieve the vision, goals and objectives outlined in the Cybersecurity Roadmap, TSA will leverage innovative cybersecurity concepts and technology that will enhance the resilience and safety of our transportation systems.

In addition to addressing key operational needs, implementing the Cybersecurity Roadmap will also enhance TSA's position as a global leader in transportation security and advance global transportation security standards.

I want to thank everyone at TSA, our interagency partners and industry stakeholders who provided input to help develop this document. It represents the beginning of an important and exciting conversation that I look forward to continuing with you as we execute the TSA Cybersecurity Roadmap.



Sincerely yours,

David P. Pekoske
Administrator

Executive Summary

TSA is charged with securing the nation's transportation systems from all threats, which involves protecting against both cyber and physical attacks. In order to meet the security demands of a constantly changing threat, TSA must ensure it is prepared to respond to cyber-related events with the same level of success that it has responded to physical threats. The TSA Cybersecurity Roadmap provides a solid framework for how TSA can operate within the cyber environment, ensure the protection of its data and information technology systems, and ensure the protection and resilience of the Transportation Systems Sector (TSS).

The TSA Cybersecurity Roadmap identifies four cybersecurity priorities and six goals that will direct TSA's efforts to improve its protection of its internal information technology systems as well as the nation's transportation systems. The National Cybers Strategy calls for the Federal Government to "develop a comprehensive understanding of national risk by identifying critical functions and will mature our cybersecurity offerings and engagements to better manage those national risks." The objectives listed in the TSA Cybersecurity Roadmap will bring TSA's cybersecurity efforts into alignment with the both National Cyber Strategy and the DHS Cybersecurity Strategy.

The TSA Cybersecurity Roadmap states that TSA will include cybersecurity in its risk and threat assessments of the TSS. As necessary, TSA will leverage existing oversight authority to conduct the assessments of stakeholder networks and contingency plans to ensure the resilience of the TSS. The Roadmap calls for TSA and our stakeholders to engage more on cybersecurity related issues. That information will include not just threat indicators and activity but also lessons learned, potential consequences, vulnerability-related details, and planning for response and recovery in the event of a cyber incident.

The TSA Cybersecurity Roadmap provides that TSA's Information Technology office (IT) will work to increase the cybersecurity of the TSA enterprise through improved governance, information security policies, and oversight. IT will also deploy innovative cybersecurity capabilities and practices to protect TSA information systems.

The TSA Cybersecurity Roadmap provides that TSA will engage the technical community within the government and private sector stakeholders to ensure appropriate prioritization of TSS equities in both federal and private sector research and development programs, with a focus on discovering vulnerabilities and in developing mitigation. This aligns with the National Cyber Strategy to prioritize national research and development interests.

The TSA Cybersecurity Roadmap will require TSA to develop agency-wide processes and policies to align agency programs and activities with this document, agency priorities, and changes in cybersecurity. TSA will also conduct an assessment of its human capital to ensure it has the appropriate levels of personnel dedicated to executing the goals and objectives identified by TSA in this Roadmap.

Table of Contents

- Introduction**..... 4
 - Scope..... 5
 - Environment..... 5
- TSA Cybersecurity Strategic Priorities** 7
 - Priority 1 – Risk Identification (DHS Pillar I)..... 7
 - Goal 1.1: Assess and Prioritize Evolving Cybersecurity Risks to TSA and the TSS..... 7
 - Priority 2 – Vulnerability Reduction (DHS Pillars II and III)..... 8
 - Goal 2.1: Protect TSA Information Systems..... 8
 - Goal 2.2: Protect TSS Critical Infrastructure 9
 - Priority 3 – Consequence Mitigation (DHS Pillars III and IV) 12
 - Goal 3.1: Respond Effectively to Cyber Incidents..... 12
 - Priority 4 – Enable Cybersecurity Outcomes (DHS Pillar V) 13
 - Goal 4.1: Strengthen the Security and Resilience of the Cyber Environment 13
 - Goal 4.2: Improve Management of TSA and TSS Cybersecurity Activities 15
- Conclusion** 16

Introduction

Protecting the nation's transportation systems to ensure freedom of movement for people and commerce is the Transportation Security Administration (TSA) mission. TSA's vision is to be an agile security agency, embodied by a professional workforce, that engages with its partners and the American public to outmatch a dynamic terrorist threat. Our nation's transportation systems, economic vitality, and security depend on a stable, safe, and resilient cyberspace. The transportation systems' cyber environment and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards. The cyber environment includes not only the interconnected network of information technology infrastructure commonly referred to as cyberspace but also the people, environment, norms, and conditions that influence that network. Sophisticated cyber actors and nation-states are developing capabilities to disrupt, destroy, or threaten the delivery of essential services. For the purposes of this roadmap, cybersecurity is defined as the practice of defending, or indirectly supporting the defense of an interdependent network of information technology infrastructure including telecommunications networks, computers, information and communications systems, and embedded processors and controllers from malicious attacks. Cybersecurity is a core mission of the U.S. Department of Homeland Security (DHS) and the Transportation Security Administration (TSA) as a component agency.¹

TSA's mission responsibilities include: (1) securing its own networks (systems, data, and security awareness and outreach), and (2) as a co-Sector Specific Agency² (SSA), working with its partners and the Transportation Systems Sector (TSS) stakeholders in coordination with DHS to secure its cyberspace. Although TSA has responsibility for oversight of both the physical security and cybersecurity of the TSS, TSA is not directly responsible for the defense of the private sector portion of TSS information technology infrastructure. Rather, TSA serves a vital role in ensuring the cybersecurity resilience of the TSS infrastructure and will work with the Cybersecurity and Infrastructure Security Agency (CISA), with its mission to protect the critical infrastructure of the United States.³ This roadmap sets forth the priorities, goals, and objectives that TSA will use to successfully execute its cybersecurity responsibilities. TSA will collaborate across the Department and will work with key federal partners and stakeholders to identify and manage national cybersecurity risks by adopting a holistic risk management approach. TSA will also work with the TSS to reduce the TSS's risk and to improve its overall resilience.

While maintaining compliance with applicable legal requirements, TSA will find innovative ways to strategically manage cybersecurity risks to its federal information technology systems and network data in addition to the TSS. Consistent with the DHS Cybersecurity Strategy, TSA has identified four priorities to increase the cybersecurity of TSA and the TSS. These priorities are:

- 1) Risk Identification (DHS Pillar I)
- 2) Vulnerability Reduction (DHS Pillars II and III)

¹ U.S. Department of Homeland Security Cybersecurity Strategy, dated May 15, 2018.

² DHS (TSA, USCG) and Department of Transportation are co-SSAs as defined in Presidential Policy Directive 21: Critical Infrastructure and Resilience (PPD-21).

³ PPD-21 defines resilience to be, "...the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. See also, Critical Infrastructure Resilience Final Report and Recommendations, 2009, National Infrastructure Advisory Council.

-
- 3) Consequence Mitigation (DHS Pillars III and IV)
 - 4) Enable Cybersecurity Outcomes (DHS Pillar V)

These four priorities align to the five DHS Cybersecurity Strategic Pillars identified in the Department of Homeland Security Cybersecurity Strategy dated May 15, 2018. Additionally, under the four TSA priorities, we have identified six goals to focus our effort and resources over the next five years. These goals are:

- 1) Assess and Prioritize Evolving Cybersecurity Risks to TSA and the TSS
- 2) Protect TSA Information Systems
- 3) Protect TSS Critical Infrastructure
- 4) Respond Effectively to Cyber Incidents
- 5) Strengthen the Security and Resilience of the Cyber Environment
- 6) Improve Management of TSA and TSS Cybersecurity Activities

By focusing on these near to mid-term goals, TSA will work to ensure the availability of transportation system functions and to foster efficiency, innovation, trustworthy communication, and economic prosperity in ways consistent with our national values and that protect privacy and civil liberties.

Scope

The TSA Cybersecurity Roadmap provides TSA with a framework directly aligned to the DHS Cybersecurity Strategy, by which TSA is to execute its cybersecurity responsibilities over the next five years. TSA will review and update the implementation plan for this roadmap on an annual basis. This document aligns TSA's Cybersecurity Strategic Priorities with the DHS Cybersecurity Strategy Pillars: I - Risk Identification; II - Vulnerability Reduction; III - Threat Reduction; IV - Consequence Mitigation; and V - Enable Cybersecurity Outcomes.

Environment

Following September 11, 2001, TSA was created to strengthen the security of the nation's transportation systems and ensure the freedom of movement for people and commerce. Today, TSA secures the nation's transportation infrastructure and vets transportation workers, commercial airline passengers and crew, and screens cargo, people, and their baggage. TSA works closely with transportation, law enforcement, and intelligence communities to set the standard for excellence in transportation security.

The threats to transportation security are continuously evolving and they are more sophisticated and more complex than ever before. TSA will use every tool at its disposal to address the associated risk and develop methods to combat them. The use of new innovative information technology will help TSA stay ahead of those who are intent on causing harm.

The proliferation of technology presents constant cybersecurity challenges and leads to significant national risks. The United States faces threats from a growing set of sophisticated malicious actors who seek to exploit cyberspace. Motivations include espionage, political and ideological interests, and financial gain. Nation-states continue to present a considerable cyber threat, while non-state actors continue to grow their own capabilities. These diverse threats can impact federal and non-federal information systems. The growing interconnectivity of cyber and physical systems within critical infrastructure creates the potential risk for malicious cyber activity to result in direct physical consequences.

While new technology alone may also help with security, it will not mitigate all of the risks and threats we are currently facing or will encounter in the future. It is critical that TSA bolster its inter- and intra-agency relationships, in addition to its engagement with external TSS stakeholders, in order to increase collaboration, communication, implementation, and development of new policies.

TSA currently supports the cybersecurity of its own networks through the Information Technology office's (IT) Information Assurance and Cybersecurity Division (IAD) under the leadership of the TSA Chief Information Officer and Chief Information Security Officer. This internal program focuses on the networks, systems, data, and outreach activities designed to secure all facets of TSA operations. It also includes some external programs such as the congressionally mandated Registered Traveler Program, which requires any commercial entity that stores data on the traveling public for the purposes of checkpoint screening activities to meet TSA's mandated baseline cybersecurity controls.

TSA is responsible for the cybersecurity of the TSS and supports it through several activities. TSA's Intelligence and Analysis office (I&A) assesses the cyber threat to the TSS. Lastly, TSA supports the TSS by providing security and mitigation guidance through several outreach and information sharing activities conducted by the Security Policy and Industry Engagement (SPIE) and the Intelligence and Analysis offices. These include participation in the Aviation Cyber Initiative (ACI), the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC), the Aviation Security Advisory Committee (ASAC), the Surface Transportation Security Advisory Committee and the Transportation Systems Sector Cyber Working Group, as well as sector-specific coordinating councils, transportation related Information Sharing and Analysis Centers (ISACs), and other working groups.⁴

TSA needs to continue to invest in people, processes and technologies to help protect its networks, systems, and data and address evolving cybersecurity risks. TSA will consider the cybersecurity mission to be a priority and focus resources to successfully execute its TSS cybersecurity outreach and coordination responsibilities with the six transportation modes under TSA's jurisdiction as a co-SSA.⁵

⁴ The Surface Transportation Security Advisory Committee is pending establishment as required by section 1969 of H.R. 302, the *FAA Reauthorization Act*.

⁵ The six transportation modes TSA is responsible for are: Aviation, Freight Rail, Highway & Motor Carrier, Pipeline, Postal & Shipping, and Mass Transit. See, Transportation Systems Sector Specific Plan of 2015.

TSA Cybersecurity Strategic Priorities

Priority 1 – Risk Identification (DHS Pillar I)

TSA will assess the cybersecurity landscape and associated risks at the strategic level to effectively allocate resources and prioritize agency efforts to address vulnerabilities, threats and consequences across all of our cybersecurity activities.

Goal 1.1: Assess and Prioritize Evolving Cybersecurity Risks to TSA and the TSS

TSA will develop a comprehensive understanding of the evolving cybersecurity risk posture to inform and prioritize risk management activities.

In order to effectively execute our mission in the long-term, we will work with stakeholders, including: (1) sector-specific agencies; (2) private sector transportation stakeholders (3) private sector cybersecurity firms; and (4) other federal and non-federal entities to gain an adequate understanding of the national cybersecurity risk posture, analyze evolving interdependencies and systemic risk, and assess changing techniques of malicious actors.

Objective 1.1.1: TSA will increase its TSS cyber domain awareness.

TSA will enhance domain awareness of the TSS through increased reporting and sharing of information of cyber-related incidents from owners and operators within the TSS. This information will include not just threat indicators and activity but also lessons learned, potential consequences, and vulnerability-related information. TSA will consider the use of regulatory measures to enhance its domain awareness of the cyber-related threats to the TSS. TSA will also consider the risk to the TSS from its interdependencies with non-regulated entities such as vendors, managed service providers, and contracted services.

Outcome: TSA has up-to-date awareness of the operations of the TSS to be able to fully execute its responsibilities as a co-SSA.

Objective 1.1.2: TSA will assess and prioritize cyber risk to the TSS and the subsectors.

TSA will incorporate cybersecurity into the risk assessments of all modes within the TSS in coordination with its federal partners and stakeholders. These risk assessments will identify the threats, vulnerabilities, interdependencies, and potential consequences of cyber incidents and attacks to the TSS. TSA's I&A will engage with government and non-government partners to ensure TSA's awareness of all transportation cyber-related incidents and intelligence. TSA's I&A will assess the cyber threat to the TSS in coordination with the Intelligence Community (IC) within the U.S. Government.

TSA's SPIE will articulate the threat to stakeholders at the classification level at which they operate. SPIE will also identify gaps in national analytic capabilities and risk management efforts across the TSS to understand the effectiveness of voluntary cybersecurity efforts. TSA will work with its federal partners, such as CISA

and the National Risk Management Center, to ensure that as cybersecurity risks within the TSS are assessed they are included and addressed in the National Strategy for Transportation Security.

Outcome: TSA is able to fully assess the range of cyber-related threats that can disrupt or destroy the TSS and TSA networks and communicate this threat effectively. TSA develops a comprehensive understanding of TSS systemic cybersecurity risks and adjusts its program and policy efforts to account for evolving technologies and operational priorities to appropriately address identified vulnerabilities and consequences.

Objective 1.1.3: TSA will assess and prioritize cyber risk to the TSA enterprise.

TSA will engage in a risk assessment of the information technology systems across the TSA enterprise and seek an understanding of trends in threats, vulnerabilities, interdependencies, and potential consequences for TSA to prioritize our cybersecurity activities, and to plan and budget appropriately. TSA will assess the cyber threat to the TSA enterprise in coordination with the Intelligence Community within the U.S. Government. TSA will also take stock of gaps in national analytic capabilities and risk management efforts within the TSA enterprise to maintain the effectiveness of our defense and resiliency of information technology.

Outcome: TSA develops an understanding of systemic cybersecurity risks to the TSA enterprise and adjusts its budgetary, resource allocation, program, and policy efforts to account for evolving technologies and operational priorities.

Priority 2 - Vulnerability Reduction (DHS Pillars II and III)

TSA will work to reduce its organizational and systemic vulnerabilities. Through technical capabilities, cybersecurity information sharing, and other outreach activities, TSS stakeholders will be empowered to better manage their cybersecurity risks.

Goal 2.1: Protect TSA Information Systems

TSA will reduce vulnerabilities to ensure TSA's network, systems, and data are secure.

TSA's Information Technology office, through leadership by its Chief Information Officer (CIO) and Chief Information Security Officer (CISO), will lead the effort to secure the agency enterprise and will use all available mechanisms to ensure that every system maintains an adequate level of cybersecurity commensurate with that individual system's risks and with those of the larger enterprise. TSA will work with the DHS CIO and CISO to ensure an adequate level of security enterprise-wide and address systemic risks and interdependencies across and between systems.

TSA will also work with CISA, to fulfill CISA's mission of protecting the .GOV domain. TSA will support efforts to reduce vulnerabilities to cyber threats by providing tailored capabilities, tools, and services to protect legacy systems as well as cloud and shared infrastructure. TSA will continue to adopt new technologies and serve as a model for other agencies in the implementation of cybersecurity best practices and enhance the security, resiliency, and reliability of the information systems across the TSA enterprise.

Objective 2.1.1: Increase cybersecurity of the TSA enterprise through improved governance, information security policies, and oversight.

To execute TSA's statutory responsibility to administer the implementation of agency information security policies and practices, TSA will continuously assess and advocate for changes to federal information technology governance structures and government-wide policies and programs that affect cybersecurity outcomes and investments. It is necessary to further refine and clarify cybersecurity roles and responsibilities based on established policies, directives, and laws that govern TSA. TSA will integrate information from existing protective capabilities along with relevant cybersecurity threat reporting from the Intelligence Community, law enforcement, and other sources. TSA will use threat reporting to enhance its ability to understand enterprise and systemic risks, inform risk management decisions, and assess potential returns on investment. Based on this information, TSA will prioritize resources to meaningfully address policy and capability gaps and build a more modern, secure, and resilient information infrastructure within TSA.

Outcome: TSA maintains an adequate level of cybersecurity commensurate with our risk within the federal enterprise.

Objective 2.1.2: Provide protective capabilities, tools, and services across the TSA enterprise.

TSA's IT office operates agency-wide cybersecurity defensive and mitigation capabilities. IT offers tools and services to assist TSA system owners to manage their cybersecurity risks. Certain elements of the agency enterprise will be further centralized to appropriately and consistently address key cybersecurity risks and provide improved security. TSA will unify the disparate networks or, as necessary, create remote monitoring/scanning capabilities to ensure uniform protection of all TSA systems governed by the Federal Information Security Management Act of 2014 (FISMA).⁶ TSA will also build on economic and operational efficiencies through the centralized purchase, or in-house development, of cyber tools and services, where appropriate, to address threats to legacy systems and cloud or shared services. TSA will undertake a systematic effort to assess its information systems at greatest risk and ensure that appropriate protective capabilities and methodologies are in place to secure sensitive information while enabling critical mission functions.

Outcome: TSA maintains a coordinated and sufficient level of cybersecurity commensurate with its own risks and with those of the government-wide enterprise to ensure the confidentiality, availability, and integrity of critical TSA information systems and information. TSA ensures that its cybersecurity approaches are flexible and dynamic enough to counter determined and creative adversaries.

Goal 2.2: Protect TSS Critical Infrastructure

TSA will partner with government and industry stakeholders to ensure that TSS cybersecurity risks are managed.

TSA will partner with its stakeholders, including co-sector specific agencies and the private sector, to drive better cybersecurity by promoting the development and adoption of best practices and industry and/or international standards. TSA will promote DHS services like risk assessments and cyber-incident response by improving engagement efforts to advance cybersecurity risk management efforts. TSA will also expand

⁶ Pub. L. 113-283, 44 U.S.C. § 3554.

operationally meaningful cybersecurity information sharing efforts to empower those protecting networks from cyber threats. While continuing to leverage existing partnership structures, TSA will deepen technical collaboration across all TSS partners, both domestic and international, on risk mitigation efforts.

To properly allocate resources and prioritize efforts, TSA will use its awareness and assessments of the cybersecurity risk posture across the TSS, as described in Goal 1.1. This includes understanding the potential consequences of infrastructure-related cybersecurity incidents and sharing of information related to cyber incidents as required by the Cybersecurity Information Sharing Act of 2015.⁷ TSA, in collaboration with DHS, will prioritize its engagement efforts based upon those with the highest risk, such as entities where a cyber-incident could result in catastrophic impacts.

Objective 2.2.1: Support and, if necessary, direct efforts to mitigate significant national and systemic cybersecurity risks to TSS critical infrastructure.

Utilizing the comprehensive understanding of cybersecurity risk to the TSS developed in Objective 1.1, TSA will collaborate with DHS, its co-SSAs, and other federal and non-federal entities to develop mitigation to cyber risks in the TSS. This will include developing tools and services for use to improve cybersecurity in the TSS, ensuring transportation specific equities are addressed. TSA will leverage these tools and services and conduct outreach to TSS owners and operators, service providers, foreign partners, and other key enablers of risk management activity. If necessary, TSA will utilize its statutory and regulatory authorities to ensure the resilience of the TSS.

Outcome: Mitigation of the most significant TSS risks to transportation infrastructure, especially those where incidents could have a significant impact on national security, public health and safety, and economic security.

Objective 2.2.2: Monitor how the TSS and the individual subsectors are implementing mitigation of cyber risks and adjust TSA guidance to the TSS as necessary.

TSA will engage TSS stakeholders on a regular basis to evaluate their implementation of guidance and to determine their cybersecurity practices and to promote resilience to malicious cyber activity. TSA will review lessons learned, potential consequences, and vulnerability-related information obtained from TSS stakeholders during cyber-related incidents. TSA will engage and assist TSS stakeholders in performing risk assessments for their respective organizations. TSA will similarly conduct a risk assessment of the TSS and update it frequently.

Outcome: TSA maintains awareness of the TSS's mitigation implementation and level of resilience to cyberattacks and cyber espionage.

Objective 2.2.3: Expand and improve sharing of cyber threat indicators, defensive measures, and other cybersecurity information.

TSA will build its capacity to assess and improve existing information sharing efforts with DHS and the TSS to ensure that the most operationally useful information is distributed for action. TSA will work with CISA to ensure cyber threat indicators and defensive measures are shared for use by TSA and distributed to TSS stakeholders as required by statute. TSA will identify and address barriers to sharing information within the

⁷ Pub. L. 114-113, 6 U.S.C. §§ 1501-1510.

U.S. Government and between agencies and international partners. This will include ensuring information about best practices, such as the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity, is available and useful for transportation cybersecurity.

TSA will collaborate with the National Cybersecurity and Communications Integration Center (NCCIC) and CISA, to engage the TSS on the use of information derived from TSS-related cyber incidents to inform and educate the TSS on cybersecurity threat indicators, defensive measures, and other best practices. This collaboration will assist in establishing a common operating picture across the TSS to assess emerging incidents and associated national, regional, or sector risks.

Outcome: TSA, after capacity development and expansion, provides coordinated sharing of relevant information with, and oversight of, the TSS cybersecurity environment. Cybersecurity stakeholders increasingly leverage information shared by TSA, DHS, and other government partners to quickly understand cybersecurity risks to TSA and TSS stakeholders, and to make timely decisions on how best to protect their information systems.

Objective 2.2.4: Improve TSA cybersecurity capabilities and resources available to TSS agencies, regulators, and policymakers.

As a co-Sector Specific Agency for the TSS, TSA will continue to develop and expand its institutional TSS knowledge and specialized expertise of cyber infrastructure for each of the subsectors (i.e., aviation, mass transit, freight rail, highway and motor carrier, and pipeline) in order to support steady-state and incident response activities in coordination with DHS and other SSA stakeholders.⁸ TSA, in conjunction with CISA, will assess the resilience of these subsectors to malicious cyber activity.

TSA will maintain relevant expertise, mature existing voluntary and regulatory partnerships, and continue to engage and coordinate cyber and physical resources for these sub-sectors. TSA will take steps to identify, recruit, and retain a workforce that is technically proficient in cybersecurity and information security and can effectively engage with industry. With its in-depth knowledge of the TSS cybersecurity environment, TSA will serve as the TSS liaison to DHS, and other relevant federal and non-federal relevant agencies as they perform their cybersecurity functions.

Outcome: The TSS is aware of its cyber risks and maintains sufficient cybersecurity-related policies and capabilities to support risk management efforts.

Objective 2.2.5: Influence vulnerability discovery and mitigation development for transportation technologies.

As a co-SSA for the TSS, TSA will engage the technical community within government and industry to ensure appropriate prioritization of TSS equities in DHS Science & Technology research and development programs, as well as private sector research and development, with a focus on discovering vulnerabilities and in developing mitigation.

Outcome: TSA has the capability to engage in the various technological disciplines for transportation at an expert level to influence these activities.

⁸ The United States Coast Guard is the SSA responsible for the Maritime Transportation Mode of the Transportation Systems Sector under the National Infrastructure Protection Plan (NIPP), which directs the Coast Guard to protect the Maritime Transportation System from cyber threats.

Priority 3 – Consequence Mitigation (DHS Pillars III and IV)

TSA will limit the impact of potentially significant cyber incidents by leveraging our emergency management expertise and insights from network protection and law enforcement efforts.

Goal 3.1: Respond Effectively to Cyber Incidents

TSA will minimize consequences from potentially significant cyber incidents through coordinated response efforts.

The ability to effectively respond to cyber incidents serves as a critical component to any organization leveraging modern technology. Under the purview of the TSA CIO and CISO, the agency manages cybersecurity incidents within its enterprise networks (commonly referred to as internal incidents) through the TSA Cybersecurity Operations Center (TSA SOC) as a component of the TSA Information Technology program office. This team monitors TSA networks for malicious activity and receives reporting from various TSA entities (employees and program offices). Once malicious activity is detected, TSA follows standard DHS reporting requirements through the Department in accordance with federal policy and law.

The National Cybersecurity Protection Act of 2014, as codified in the Homeland Security Act, mandated that DHS, through CISA and the NCCIC, serves as the federal civilian interface for sharing information related to cybersecurity risks, incidents, and warnings for federal and non-federal entities, such as the stakeholders that make up the TSS.⁹ In accordance with Presidential Policy Directive Number 41 – United States Cyber Incident Coordination, TSA, in coordination with CISA, is prepared to provide the TSS specialized expertise to support the needs of federal responders and promote and support private TSS coordination during and after a cyber-incident.¹⁰

TSA will proactively engage with our federal partners and the TSS before incidents occur. In the case of significant cyber incidents, TSA must be prepared to contribute its specialized expertise to coordinated government-wide responses and to support any related emergency management activities. TSA will also ensure that we have mechanisms in place to coordinate with international partners to respond to cyber incidents, whether a cyber-related incident originates domestically or abroad.

Objective 3.1.1: Increase incident reporting and victim notification to facilitate response assistance.

The TSA SOC will lead all cyber incident response and management activities for the TSA enterprise, networks, and data, and will be leveraged as TSA's central reporting point for cyber incidents.

TSA cybersecurity efforts will continue to build trusted relationships with TSS entities at greatest risk of experiencing potentially significant cyber incidents. TSA will establish reporting guidance for the TSS stakeholders in alignment with the NIST Cybersecurity Framework, the National Cyber Incident Response Plan, and the Cybersecurity Information Sharing Act of 2015.¹¹ TSA, in coordination with CISA will also develop protocols for sharing information from cyber-related incidents with foreign government officials.

TSA will ensure that the Transportation Security Operations Center (TSOC) is adequately prepared to receive cyber-related incident reports from regulated and non-regulated stakeholders. TSA, through its appropriate

⁹ The National Cybersecurity Protection Act of 2014. Public Law 113-282. (December 18, 2014). *See also*, 6. U.S.C. § 149.

¹⁰ PPD-41 issued July 26, 2016.

¹¹ Pub. L. 114-113, 6 U.S.C. §§ 1501-1510.

internal offices, will share information from these incident reports with its federal partners, such as CISA; international partners, in coordination with CISA; and TSS stakeholders. TSA will enhance domain awareness of the TSS through increased reporting and sharing of information of cyber incidents from owners and operators, including lessons learned, potential consequences, and vulnerability-related information. This information will include not just threat indicators and activity but also lessons learned, potential consequences, and vulnerability-related information.

TSA will continue to develop its relationships with federal partners to ensure that TSA has the situational awareness necessary to communicate effectively with the TSS. A culture of reporting, notification, and information sharing will: (1) increase the security and resilience of critical infrastructure; (2) help prevent, counter, and disrupt illicit cyber actors; and (3) enable the Federal Government to assess and potentially manage responses to cyber incidents within the TSS.

Outcome: TSA receives reports of internal cyber-incidents and communicates them to the TSA SOC. TSA receives reports of external cyber-incidents, which are communicated to the NCCIC and makes timely notifications to the TSS as appropriate. Information from external cyber-incidents is incorporated into TSA's risk assessments of the TSS.

Objective 3.1.2: Expand asset response capabilities to mitigate and manage cyber incidents.

TSA will develop a coordinated response capability for internal and external cyber incidents. TSA will coordinate the response to cyber incidents for TSA systems and/or network specific events with the DHS Enterprise Security Operations Center. TSS cyber incidents will be coordinated with co-SSAs to support DHS asset response. TSA is prepared to receive and contribute to shared situational awareness of emerging cybersecurity risks and incidents impacting the TSS and/or the agency. As required by PPD-41, during significant cyber incidents, TSA must be prepared to fully participate in and support the Cyber Unified Coordination Group and the White House-led Cyber Response Group for cyber incidents impacting TSS equities.

Outcome: TSA responds to cyber incidents by providing coordinated agency response and assistance, where requested and appropriate, and supporting DHS asset response and national-level decision-making and emergency management efforts.

Priority 4 - Enable Cybersecurity Outcomes (DHS Pillar V)

TSA will enable improved cybersecurity risk management outcomes by supporting federal IT security policy and TSS operational efforts that make the Transportation Systems Sector more secure and reliable. These efforts help shift the advantage away from malicious cyber actors toward those protecting cyberspace. TSA will similarly look internally to align our efforts to maximize cybersecurity outcomes.

Goal 4.1: Strengthen the Security and Resilience of the Cyber Environment

TSA will enhance continuous awareness and preparedness by promoting voluntary, collaborative, and sustainable community action.

A more fundamentally secure cyber environment can help tip the balance toward those protecting networks and away from malicious cyber actors. Strengthening the security and reliability of the cyber ecosystem therefore enables risk management and sets the conditions to support other TSA strategic cybersecurity goals.

TSA will support efforts across the TSA enterprise and the TSS that will result in fundamentally improved security outcomes through technological innovation as well as the widespread adoption of improved operational and policy frameworks. TSA will develop collaborative communities, build global partnerships, and participate in international and multi-stakeholder venues to advance positive developments in cybersecurity. TSA will leverage DHS' expansion of cyber personnel programs to assist with strengthening and increasing the reliability of the cyber environment.

Objective 4.1.1: Enhance international collaboration to promote an open, interoperable, secure, and reliable TSS cyberspace.

TSA international cybersecurity engagements will help shape the TSS cyber environment to support TSA's cybersecurity objectives and broader U.S. foreign policy priorities. TSA will develop and maintain relationships with international organizations, such as the International Civil Aviation Organization (ICAO), and other international partners that advance our specific transportation security-related objectives and expand on comprehensive planning for a secure cyberspace. TSA will engage with its international partners to understand their cybersecurity goals and requirements to ensure the scope of the TSA engagement and oversight of the TSS strengthens the security and reliability of the TSS cyber environment.

TSA will clearly articulate further entrance processes for sharing cyber threat information with foreign transportation entities, as well as which foreign transportation entities will receive it. TSA will collaborate with foreign transportation stakeholders to develop cyber threat information sharing agreements that provide clear guidance on distribution and use of the threat information.

TSA will work with DHS, the IC, and other relevant partners within the U.S. government to develop policy, where needed, to share TSS-related information with relevant foreign government and private sector entities.

Outcome: TSA international engagements result in shared global approaches and standards to the Transportation Systems Sector cybersecurity, as well as increased cooperation on cybersecurity risk management activities.

Objective 4.1.2: Improve staffing, recruitment, education, training, and retention to develop a world-class cyber workforce.

TSA will use its unique statutory hiring authority under the Aviation and Transportation Security Act to recruit highly qualified candidates to TSA and will continue to support efforts to increase the supply of national cybersecurity talent through cyber education programs, such as the National Initiative for Cybersecurity Education. TSA will also continue to develop and promote cybersecurity training programs dedicated to advancing the cybersecurity skills of its existing federal workforce. TSA will leverage DHS' cyber-personnel initiatives on personnel recruitment, training, and retention efforts which enable hiring and compensation flexibilities.

Outcome: TSA staffs, recruits and trains highly-skilled cybersecurity personnel and develops a cadre of well-trained cybersecurity professionals.

Goal 4.2: Improve Management of TSA and TSS Cybersecurity Activities

TSA will execute our agency cybersecurity efforts through a single coordinated, integrated, and prioritized process.

Each of the cybersecurity goals identified in this roadmap involve multiple TSA offices. While some have major external responsibilities with respect to network protection or law enforcement, all are involved in protecting TSA IT systems and data. To ensure agency-level unity of effort and a coordinated approach to accomplishing our cybersecurity goals and objectives, TSA will continually assess evolving risks and evaluate priorities in the cybersecurity mission space. TSA will align agency programs and activities with this roadmap, agency priorities, and changes in cybersecurity. TSA will also assess its human capital to ensure it has the appropriate levels of personnel dedicated to executing this roadmap.

Objective 4.2.1: Integrate agency-wide cybersecurity policy development, strategy, and planning activities and align TSA activities with Department-wide activities.

TSA will develop clear roles and missions across the TSA enterprise for cybersecurity through a cybersecurity Management Directive and develop the capacity to accomplish these roles and missions. TSA will work with the DHS Office of Policy, CISA, DHS's Office of Intelligence and Analysis, as well as its federal partners in the U.S. intelligence and law enforcement communities, to ensure the development and execution of consistent, integrated cybersecurity policies and strategic plans.

Outcome: TSA executes our cybersecurity mission responsibilities in a coordinated and integrated manner between all offices within TSA.

Objective 4.2.2: Prioritize and evaluate the effectiveness of TSA cybersecurity programs and activities.

TSA will ensure that its cybersecurity programs and activities align to the goals and objectives set forth in this roadmap. TSA will leverage management processes to evaluate programs and activities to assess their effectiveness and to ensure that program funding, personnel, and other resources are optimized to meet Departmental priorities. TSA will engage in a review of its human capital assets to ensure that it has the appropriate staffing levels across TSA to review and execute its cybersecurity related policies and regulations.

Outcome: The TSA cybersecurity program effectively and efficiently addresses departmental goals and objectives.

Conclusion

TSA will develop and maintain a leadership role, collaborating with other federal departments and agencies, the private sector, and other stakeholders, to ensure that cybersecurity risks are effectively managed, critical networks are protected, vulnerabilities are mitigated, cyber threats are reduced and countered, incidents are responded to in a timely and effective way, and the TSS cyber environment is secure and resilient. Meeting the goals and objectives outlined in this roadmap requires a unified, near to mid-term approach. Aligning network protection authorities with traditional risk management, information sharing, and incident response efforts will enhance TSA cybersecurity efforts moving forward.



Transportation Security Administration



@TSA



@TSA



v/TSA/