Insider Threat Roadmap 2020

Transportation
Security
Administration

Administrator's Message

I am proud to present the Transportation Security Administration's (TSA) Insider Threat Roadmap. This document provides a vision to guide TSA and the transportation community in mitigating insider threat. It builds on the expertise, leadership, and relationships we have developed to streamline processes, identify requirements and capabilities, and leverage partnerships to proactively mitigate risks associated with the insider. I acknowledge that publishing this roadmap during the COVID-19 National Emergency may present a challenge, and we intend to carefully coordinate and plan implementation with our stakeholders and security partners as the nation recovers.

The Insider Threat Roadmap defines the common vision for the Transportation Systems Sector that insider threat is a community-wide challenge, since no single entity can successfully counter the threat alone. It aligns with and supports the 2018-2026 TSA Strategy and the 2020 National Strategy for Transportation Security, and builds on standards established by the National Insider Threat Task Force.[1] The Roadmap also addresses a GAO-20-275SU Report recommendation, dated February 2020, to develop and implement a strategic plan that includes strategic goals and objectives.

To achieve the vision, priorities and objectives outlined in the Insider Threat Roadmap, we will work with our interagency partners and industry stakeholders to refine and improve efforts to detect, deter, and mitigate insider threats, leveraging innovative concepts and technology to enhance the resilience and safety of our transportation systems. In addition to addressing key operational needs, implementing the Insider Threat Roadmap will also enhance our position as a global leader in transportation security and advance global transportation security standards.

I want to thank everyone at TSA, our partners and stakeholders who provided input to help develop this document. It represents the next step in an important and exciting conversation that I look forward to continuing with you as we execute this strategic plan.

Sincerely yours,

David P. Pekoske

David P. Pekoske
Administrator

[1] Executive Order 13587

Executive Summary

TSA, in its mission to protect the nation's transportation systems to ensure freedom of movement for people and commerce, faces a range of growing challenges associated with insider threats. TSA's responsibility for insider threat mitigation extends throughout the Transportation Systems Sector (TSS). We believe this is a community-wide risk and this document establishes a holistic approach to mitigation that requires broad stakeholder participation to detect, deter, and mitigate this risk.

This Insider Threat Roadmap provides a vision to guide TSA and the transportation community in mitigating insider threat. The Roadmap builds on the expertise, leadership, and relationships TSA has developed to streamline processes, identify requirements and capabilities, and leverage partnerships to proactively mitigate risks of the insider threat. It builds on and supports DHS Directive 262-05-002, "*Information Sharing and Safeguarding: Insider Threat Program*," issued on October 1, 2019, which establishes requirements and standards, and assigns responsibilities for DHS agencies to implement an insider threat detection and prevention program.

For the purposes of this roadmap, we define Insider Threat as the threat that *an individual with authorized access to sensitive areas and/or information, will wittingly or unwittingly misuse or allow others to misuse this access to exploit vulnerabilities in an effort to compromise security, facilitate criminal activity, terrorism, or other illicit actions that inflict harm to people, organizations, the transportation system, or national security.*[2]

The insider threat landscape is dynamic and the capabilities associated with it continue to evolve. TSA has consistently identified insider threat among its enterprise-level risks.[3] As recently as 2019 terrorists have sought to leverage insiders to conduct attacks on the transportation system. There are concerns that terrorists could exploit the tactics, techniques, and procedures used by transnational criminal organizations to identify and recruit, or develop and emplace insiders into the TSS.

TSA's approach is to continue refining and improving efforts to detect, deter, and mitigate insider threats to transportation sector personnel, operations, information, systems and critical infrastructure. TSA seeks to identify and exploit long-term trends and patterns associated with insider threats and has developed the Insider Threat Roadmap to guide its and the transportation communities' holistic efforts to detect, deter and mitigate this risk. TSA will:

1) Promote meaningful data-driven decision making to **detect** threats by:
   - Collecting and using threat information better, and
   - Developing and maintaining technical capabilities to identify and evaluate risk indicators
2) Advance operational capability to **deter** threats by:
   - Optimizing information to improve capabilities, and
   - Enhancing insider threat detection and case management

[2] Definition adapted from the ASAC Report on Insider Threat at Airports, dated 7/19/18
[3] Transportation Security Administration, *TSA Enterprise Risk Register* (May 2019)

3) Mature the capability of the Transportation Systems Sector to **mitigate** threats by:

- Fostering an agile insider threat posture, and
- Partnering with stakeholders to create tailored mitigation strategies.

Achieving these priorities will ultimately foster and sustain a robust security culture and mindset where insiders take responsibility for their actions and those of their coworkers operating in the TSS. The Insider Threat Roadmap requires TSA to develop agency-wide processes and policies to align agency programs and activities with this document, agency priorities, and changes in standards. TSA will also conduct an assessment of its human capital and resources to ensure it has the appropriate levels of personnel dedicated to executing the goals and objectives identified by this Roadmap.

Table of Contents

Introduction

Demand in all modes of transportation can be dynamic, though it typically increases annually. As the Transportation Systems Sector (TSS) adjust to volume changes, the opportunity and potential of insiders grows. TSA has embraced a holistic approach to insider threat mitigation to address these challenge, and it is essential that transportation interagency partners and private sector stakeholders share a common view of insider threat as a community-wide challenge.

TSA began conducting counter insider threat activities early in its existence and established a formal program in 2013. Executive Order 13587, "*Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*," issued by the White House on October 7, 2011, requires all federal agencies that operate or access classified computer networks to establish an insider threat detection and prevention program. The order established the National Insider Threat Task Force (NITTF). The "*National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*," issued by the White House in November 2012, provides executive branch departments and agencies with the minimum elements necessary to establish functional insider threat programs. DHS Directive 262-05-002, "I*nformation Sharing and Safeguarding: Insider Threat Program*," issued on October 1, 2019, establishes requirements and standards, and assigns responsibilities for DHS agencies to implement an insider threat detection and prevention program.

Insider threat can manifest as damage to TSA and the TSS through the following examples of insider behaviors:

- Terrorism, or extremist activities directed against TSA, the TSS, or other critical or populous targets using the TSS as a means to do harm
- Sabotage
- Subversion
- Smuggling of persons or contraband
- Corruption, to include participation in transnational organized crime
- Attempted or actual espionage
- Unauthorized access to security restricted areas and information
- Unauthorized disclosure of information
- Conspiracy to commit a criminal offense
- Workplace violence

TSA applies a layered approach to securing the traveling public and the nation's transportation systems. Each layer is intended to deter, detect, and mitigate a terrorist attack. This combination multiplies their security value, creating a much stronger, more dynamic system. An insider who has to overcome multiple security layers to carry out an attack is more likely to be pre-empted, deterred, or defeated during the attempt. Insider threat defense is an important aspect of TSA's layered strategy of overall transportation security. Efforts to counter insider threats require collaboration among TSA, federal partners, law enforcement, state and local authorities, and industry stakeholders, including transportation workers. TSA continues to work with these stakeholders to advance insider threat security standards, including insider threat countermeasures.

Enhancing cooperation with international partners is another key enabler for protecting the United States beyond its shores and the broader TSS against the insider threat. The United States will continue to work with foreign partners to improve transportation security worldwide, through cooperation to enhance international standards and best practices, and harmonize regulations and enforcement measures. This will include initiatives pursued through private sector participation within international organizations.

Purpose and Vision

Purpose: Mitigate the risk posed by insider threats to TSA and the Transportation Systems Sector.

Vision: A mature, collaborative program that comprehensively and continuously identifies and mitigates insider risk to TSA and the Transportation Systems Sector.

Strategic Environment

The strategic environment describes the broad range of factors that influence our understanding of operational conditions. It is an assessment of the set of conditions, circumstances, and influences that drive insider threat in the transportation sector. The insider threat landscape is dynamic and the capabilities associated with it are evolving exponentially. These factors, along with economic and sociological pressures, may make insiders possessing specialized technological skills a potential threat to the TSS.

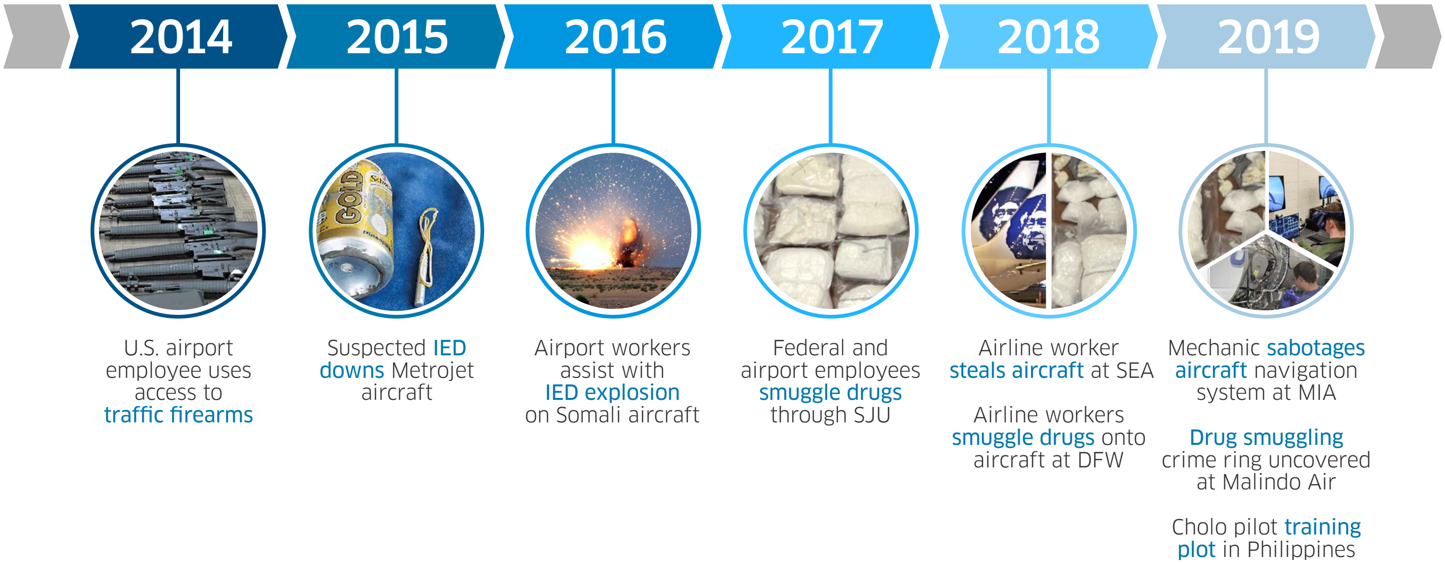
Operational Factors

TSA will assess the operational 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 insider threat activities.

- **Volume.** Terrorist organizations seek to infiltrate organizations using insiders. As the transportation sector grows in size and complexity, so do the number and types of potential insiders.
- **Technology.** Technological change increases the number of threat vectors an insider can exploit to cause harm, wittingly or unwittingly. Individuals possessing the skill and expertise to exploit technology are becoming more sophisticated, facilitating their ability to exfiltrate information from automated systems. Even traditional threat actors can be assisted or amplified by technology. Technology, however, can also be used to mitigate this factor.
- **Rapid Radicalization.** Self and rapid radicalization, and other motivations, may make insider activity more difficult to detect and mitigate.
- **Shared Environment.** The TSS is complex, encompassing commercial operators, public agencies, third-party providers, and supply chains accomplishing or supporting movement of high volumes of people and commodities essential to our nation’s economic well-being and national security. Overlapping authorities, responsibilities, and missions mean that cooperation and collaboration in countering insider threats are integral in a layered approach to transportation security. For this purpose, many owner/operator organizations and entities in supporting industries maintain insider threat programs or similar initiatives tailored to their mission, operating environment, and organizational culture. The private sector is typically more agile, based on legal, privacy, and other reasons to rapidly implement insider threat activities. TSA’s vision is to support these tailored efforts through complementary policies, programs, and procedures.
- **Facilitation of Commerce.** TSA’s primary mission is to protect the nation’s transportation systems to ensure freedom of movement for people and commerce. Insider threat mitigation measures must be effective and efficient to support this mission and allow the continued efficient movement of people, goods, and commodities in all modes of transportation. Measures must not be so cumbersome as to cause a significant and unwarranted disruption of legitimate commercial activity, and must consider the privacy and civil liberties of travelers and transportation workers.

Threat Assessment

Insider threat activity in the TSS has generally been related to industrial sabotage, theft, and/or smuggling rather than terrorism, but, as recently as 2019, terrorists have sought to leverage insiders to conduct their attacks. There are valid concerns that terrorists could exploit the tactics, techniques, and procedures used by transnational criminal organizations to identify and recruit, or develop and emplace insiders into the TSS. The incidents below highlight high-risk insider activity within the TSS.



2014
U.S. airport employee uses access to traffic firearms

2015
Suspected IED downs Metrojet aircraft

2016
Airport workers assist with IED explosion on Somali aircraft

2017
Federal and airport employees smuggle drugs through SJU

2018
Airline worker steals aircraft at SEA

Airline workers smuggle drugs onto aircraft at DFW

2019
Mechanic sabotages aircraft navigation system at MIA

Drug smuggling crime ring uncovered at Malindo Air

Cholo pilot training plot in Philippines

- In July 2019, a U.S. airline mechanic sabotaged a navigation system of a 737-800 aircraft at Miami International Airport. The mechanic admitted to investigators that he tampered with an exterior compartment of the aircraft and glued a piece of foam to the air data module. Security camera footage indicates that the suspect accessed the compartment in question during the incident.
- In 2019, a flight attendant was arrested for allegedly smuggling $14.5 million worth of drugs into Australia from Malaysia as part of a Vietnamese crime ring. The 38-year-old suspect reportedly hid the drugs on his body and in his luggage while working for Malindo Air, a subsidiary of Indonesian-based Lion Air. The crew member and seven others were arrested in and around the Melbourne area.
- In 2019, an individual linked to a terrorist group was training to become a pilot, with probable nefarious intent. Philippine authorities arrested Cholo Abdullah, an alleged member of the al-Qaida-linked al-Shabaab terrorist group, who was attending pilot training at an aviation academy in Manila, Philippines. Abdullah had reportedly researched aviation threats, aircraft hijacking, and falsifying travel documents.
- In 2018, after successfully clearing through an employee inspection checkpoint at Seattle-Tacoma International Airport (SEA), an airline worker used his access to steal a Horizon Air passenger aircraft and fly it for approximately 70 minutes before crashing on Ketron Island, 25 miles southwest of SEA. There were no additional passengers on board and the airline worker did not survive the crash.
- In 2018, a network of airline workers were arrested at Dallas Fort Worth International Airport (DFW) for using their access to bypass airport security measures and smuggle drugs onto departing passenger aircraft.

- In 2017, six federal government employees, airport security personnel, and a ramp employee smuggled suitcases, each containing cocaine, through the TSA security system at San Juan Luis Muñoz Marín (SJU) Airport and onto commercial aircraft without detection.
- In 2016, a transit authority police officer for a mass transit agency in a U.S. city was arrested and charged with intentionally providing material support and resources to the Islamic State of Iraq and the ash-Sham (ISIS) from 2014 through 2016. Although the law enforcement investigation did not reveal any information regarding specific attack planning against the Homeland or direct communication with ISIS, this incident highlights the potential threat posed by an insider—in this case a law enforcement officer—to domestic rail operations and infrastructure.
- In 2016, shortly after takeoff, an explosion occurred onboard a passenger aircraft traveling from Somalia. Somali intelligence officials say two airport workers handled a laptop containing a bomb that later exploded in the passenger aircraft. A video shows one airport worker handing the laptop to another employee. The two then hand the laptop over to a man who was later killed when the laptop exploded prematurely.
- In 2015, shortly after takeoff, Metrojet Flight 9268 was downed over the Sinai Peninsula, by a suspected Improvised Explosive Device (IED) placed in the cargo hold, killing all 224 persons onboard.
- In 2014, an airport employee was arrested and charged with trafficking firearms and entering secure areas of a U.S. airport in violation of security requirements. The employee repeatedly evaded airport security with bags of firearms, some of which were loaded. The employee then passed the guns off to an accomplice who transported them as carry-on luggage to another domestic location, where they were illegally sold.

These incidents, and other similar cases, highlight tactics, techniques, and procedures employed by drugs or arms smuggling insiders – exploiting insider access to bypass security measures – that could be replicated by terrorist insiders. Common techniques employed in numerous, but not all, smuggling events include: 1) insiders conspiring; 2) insiders transporting prohibited items in hand-carried containers such as backpacks or carry-on luggage; 3) insiders carrying dangerous or prohibited items into a security restricted area; and 4) insiders passing prohibited items they smuggled through access points to witting passengers in the security restricted area, particularly in locations without closed-circuit television surveillance camera monitoring.

Guiding Principles

In implementing the objectives outlined in this document, TSA will apply the following guiding principles. These principles describe how we operate to make this insider threat mitigation vision a reality and how we use the roadmap to navigate the risk terrain.

- **Create operational efficiencies that allow for reinvestment in security.** TSA, in coordination with security partners and stakeholders, will seek to improve its performance efficiency, which will allow for budgeting flexibility. Technology can enable organizations to automate current manual procedures and reinvest resources into other critical security tasks.

- **Promote a security culture.** TSA will promote and incentivize a sustainable security culture where insiders take responsibility for their own actions and for the actions of their coworkers. Insiders need to know they are responsible and accountable for their actions and will be recognized for their positive contributions to security.

- **Safeguard individuals' privacy and civil liberties.** TSA will adopt a "privacy-by-design" mindset that incorporates Privacy Act requirements and civil liberty considerations into each phase of security program development.

- **Achieve Unity of Effort Across DHS and the TSS.** TSA will work with the transportation industry to harmonize efforts among multiple organizations working towards a similar objective. TSA intends to pursue innovative models of public-private partnerships to drive collaboration and shared investment to establish the best route to unlocking a business case for an effective insider threat program. At the same time, TSA and our partners must work to clearly articulate public and private sector roles and responsibilities in the context of applicable laws and regulation.

- **Be Adaptive and Resilient.** TSA's insider threat capabilities must adapt to an ever-evolving risk environment and we must embrace change with optimism and resilience, and encourage a culture of agility. TSA will collaborate with its federal partners and industry stakeholders to develop effective security measures and solutions using an iterative approach. This approach encourages frequent review and adaptation to adjust to changing realities and threats, yet allows organizations to continue using and improving existing best practices.

Strategic Priorities

TSA aims to achieve its insider threat vision for the TSS by advancing three overarching priorities in parallel.

Priority 1: Promote Meaningful Data-Driven Decision Making

Priority 2: Advance Operational Capability

Priority 3: Mature the Capability of the Transportation Systems Sector

Establishing the Foundation: Ensure full operational capability of the NITTF Minimum Standards

TSA will continually assess its security posture and performance against the national programmatic standards established by the NITTF *2017 Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards*, as well as progress toward optimizing program capabilities as stated in the Insider Threat Program Maturity Framework (2018). The Insider Threat Roadmap describes how TSA will move beyond this baseline and continually examine ways to make its programs more effective in deterring, detecting, and mitigating insider threat and become more efficient in conducting daily operations.

Priority 1: Promote Meaningful Data-Driven Decision Making

Crucial to mitigating insider threat activity is the information needed to detect it. Specifically, accurate and quality source information is key to effectively inform mitigation activities. This priority is intended to align existing information and data sources, ensure their integrity, and use them for modeling and analysis.

Objectives:

1.1 Prioritize high value key assets and mission critical functions

To effectively execute our mission over the long-term, we will work with our security partners and stakeholders to determine key asset priorities and critical functions from the perspective of the risk of the insider – elements that are essential to operations and to national security and which, if damaged, stolen, or otherwise exploited, would have a damaging effect on the organization, its mission, and national security.

1.2 Develop and maintain insider threat risk indicators

Risk indicators, whether they be behavioral, physical, technological, or financial can expose malicious or potential malicious insiders to detection. TSA and its security partners and stakeholders will identify and assess key indicators to assist with evaluation and identification of insider threat and to inform the development of effective mitigation strategies across the TSS. We will review insider threat cases for the purposes of identifying patterns or trends of significance, especially for indicators of developing threat. TSA will increase its profile as a source of information on the types of behaviors and actions that have occurred in actual insider threat incidents to inform awareness, preparedness, and risk mitigation measures.

1.3 Model the probability of factors that influence insider threat

We will improve the TSS's ability to detect potentially malicious insiders by implementing comprehensive solutions encompassing advanced empirical models, improved information/intelligence sharing, and threat detection. Advanced analytic solutions (e.g., artificial intelligence, probabilistic analytics, data mining) will help develop insider threat screening and staffing models to best allocate resources and deploy mitigation measures.

1.4 Identify disparate information sources

We will establish a structured approach to gathering insider threat information that will inform insider threat analysis. We must identify key information sources, and ensure they are accurate and available for use in informing risk mitigation activities.

1.5 Mature a case management capability that automatically ingests and synthesizes information

Insider threat programs depend on collaboration among multiple offices and the synthesis of many disparate information sources. We will develop capabilities to synthesize data and risk information to support TSA and industry insider threat mitigation activities.

Priority 1 Outcome: TSS has the capability to collect and synthesize information and assess key indicators to estimate the chance of an insider threat and detect insider threats.

Priority 2: Advance Operational Capability

TSA will partner with federal agencies, state and local authorities, and the private sector to drive better insider threat management by promoting the development and adoption of best practices and industry and/or international standards. We will promote resources like the NITTF[4] and its reference materials for federal departments and agencies to develop, implement, and enhance insider threat mitigation programs. In collaboration with stakeholders, we will identify areas where many concepts and "best practices" can be adapted and applied in the TSS. While continuing to leverage existing partnership structures, we will deepen collaboration across the TSS, both domestically and internationally, on risk mitigation efforts.

To properly allocate resources and prioritize efforts, we will use our awareness and assessments of the insider threat posture across the TSS. This includes understanding the potential consequences of infrastructure-related insider threat incidents and the sharing of information related to such incidents. TSA will prioritize its engagement efforts based upon those areas with the highest risk, such as environments where an insider threat incident could result in catastrophic consequences.

Objectives:

2.1 Establish a unified operational approach

We will develop joint operations plans for insider threat mitigation that identify response protocols, roles, responsibilities, and activities contributing to a unified community effort.

[4] NITTF, co-directed by the FBI and the National Counterintelligence and Security Center, was established in October 2011 by Executive Order 13587, which directed federal departments and agencies with access to classified information to establish insider threat detection and prevention programs. The NITTF was established to assist agencies in developing and implementing these programs. More information can be found at https://www.dni.gov/index.php/ncsc-how-we-work/ncsc-nittf

2.2 Establish an enterprise-level, centrally managed capability to integrate, analyze, and respond to potential insider threat information

We will establish an Insider Threat Mitigation Hub to elevate insider threat to the enterprise level and enable multiple offices, agencies, and industry entities to share perspectives, expertise, and data to enhance threat detection, assessment, and response across the TSS. This capability will allow us to fuse together disparate information points to identify intricate patterns of conduct that may be unusual or indicative of insider threat activity and drive enhanced insider threat mitigation efforts.

2.3 Reduce our organizational and systemic insider vulnerabilities through enhanced policies, technical capabilities, information sharing, and other activities

TSA will work with TSS stakeholders to promote and incentivize a collective security culture and mindset where insiders take responsibility for their actions and for those of their colleagues. Wherever possible, we will support efforts to reduce insider vulnerabilities by providing tailored capabilities, tools, and services. We will continue to revise processes, adopt new technologies and serve as a model for other agencies in the implementation of insider threat mitigation best practices.

2.4 Collect and analyze data on insider threat program compliance

We will work with our security partners and stakeholders to understand the effectiveness of and improve on insider threat programs. We will seek to determine the level of compliance and governance needed for an organization to “self-police.”

Priority 2 Outcome: TSA and the TSS leverage comprehensive insider threat information and analyses to react to threats, and manage vulnerabilities and consequences by enhancing deterrence, detection, and mitigation capabilities.

Priority 3 – Mature the Capability of the Transportation Systems Sector

Insider threat best practices and industry standards should be disseminated enterprise-wide and key stakeholders engaged to boost their adoption. TSA will enhance continuous awareness and preparedness by promoting voluntary, collaborative, and sustainable community action. We will support efforts across the TSA enterprise and the TSS that will benefit from fundamentally improved security outcomes through technological innovation as well as the widespread adoption of improved operational procedures and policy frameworks. TSA will develop collaborative communities, build global partnerships, and participate in international and multi-stakeholder venues to advance positive developments in insider risk mitigation.

Objectives:

3.1 Establish a TSS Insider Threat maturity framework that raises the security baseline

Insider threat is a dynamic problem – the threat landscape is constantly evolving, technology is rapidly shifting, and organizations are changing in response to various pressures. Our collective efforts to address insider threat require agility, with constant evaluation, fresh perspectives, and updated approaches to address current and future risk. We will work with our partners and stakeholders to progress toward optimizing insider threat program capabilities. TSA will establish a formal program review cycle to adjust to changing threats, assess performance, and establish a virtuous refresh and investment cycle.

3.2 Seek technology that improves detection and mitigation

We will pursue research, development, testing, and evaluation of technologies that identify and validate solutions to augment detection and mitigation capabilities. We will incentivize private sector acquisition of improved technology with periodic refresh cycles and will work to align with private sector business decision cycles.

3.3 Develop testing protocols

We will enhance and integrate capabilities for testing to inform vulnerability analysis and the continuous improvement of mitigation measures. TSA will engage with stakeholders in exercises to prepare for insider incidents and test the effectiveness of security programs by identifying gaps in their preparedness measures.

3.4 Share what works by implementing an information sharing platform, training programs, and processes for lessons learned and best practices

We will enhance domain awareness through timely delivery of relevant intelligence, information, and training products for the transportation industry to implement mitigation strategies to reduce risk. We will identify ways to share insider risk information with the private sector through public-private partnerships using data sharing architecture, modeling, and data analytics to better identify and mitigate insider risk. We will establish an engagement approach and educational curriculum on insider threat management for organizations within the TSS. TSA will establish processes to assess, integrate, and share lessons learned, and industry and government practices.

3.5 Leverage and promote insider threat practices throughout the supply chain

It is important to build security measures and expectations into any service agreements with third-party providers that have physical access to key assets and functions. We will collaborate with the transportation industry to promote vertical integration[5] of insider threat mitigation practices and processes.

3.6 Minimize consequences from potentially significant insider incidents through coordinated response efforts

We will develop a coordinated response capability for internal and external insider incidents. Insider incidents will be coordinated with federal partners to support DHS asset response. TSA is prepared to receive and contribute to shared situational awareness of emerging insider threats and incidents impacting the TSS and/or the agency.

Priority 3 Outcome: The transportation sector insider threat posture is agile and our layered program performance is optimized and measured on a continuous improvement cycle.

[5] Vertical integration in this context means that the transportation providers work with their vendors, suppliers, and supporting companies to adopt insider threat programs and practices.

Path Forward

TSA will develop implementation plans that include management approaches, timelines, and performance measures to assess progress with each of the strategic priorities and objectives in this roadmap.[6] These implementation plans will capture detailed plans of action. Recognizing there is no 'turn-key' solution to mitigating insider threat, TSA and its security partners and stakeholders will take a phased approach to implementation that incrementally raises the security baseline. This approach is intended to enable us and our partners to be agile and to iteratively build capability in accordance with applicable laws, authorities, and privacy considerations.

[6] GAO-20-275SU Report recommendations

U.S. DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

@TSA @TSA facebook.com/TSA/