



# Annual Report on Transportation Security

Fiscal Year 2022 Report to Congress  
October 10, 2024



[tsa.gov](https://tsa.gov)

# Message from the Administrator

October 10, 2024

I am pleased to submit the “Annual Report on Transportation Security” prepared by the Transportation Security Administration (TSA). This report summarizes activities and accomplishments during Fiscal Year (FY) 2022 by transportation system owners and operators, and federal, state, local, tribal, and territorial government partners to protect and enhance the resiliency of our Nation’s transportation systems. This report, based on reporting requirements,<sup>1</sup> provides updates on the implementation of modal security plans<sup>2</sup> and highlights some of the many initiatives conducted in pursuit of the TSA mission.



The security of our Nation’s expansive and complex transportation systems is rooted in our strong partnerships with both industry and government stakeholders. The efforts of the Transportation Systems Sector (TSS) is enriched by a diverse community of talented security professionals, directly reflected through the work of TSA’s frontline workforce at airports; the groups working behind the scenes to analyze information, conduct research, and test and implement advanced technologies; and, in the efforts of industry and government leaders. These leaders regularly come together to engage in discussions, share information and current best practices; conduct exercises; participate in assessments; develop recommendations; and work to effect pragmatic policies and regulations aligned with the ever-evolving transportation landscape. Through the efforts of a unified transportation sector, we will continue to mitigate, outmatch, and overcome threats that would otherwise attempt to compromise our precious freedoms.

TSA is the lead federal agency for transportation security, and shares responsibility with the U.S. Coast Guard (USCG) and the Department of Transportation (DOT) as co-Sector Risk Management Agencies (co-SRMAs). Other Components in the Department of Homeland Security (DHS) that have transportation sector security responsibilities include U.S. Customs and Border Protection (CBP), Cybersecurity and Infrastructure Security Agency (CISA), and Countering Weapons of Mass Destruction Office (CWMD).

---

<sup>1</sup> 49 U.S.C. § 114(s)(4)(B); 49 U.S.C. § 44938(a); Section 109(b) of the Aviation and Transportation Security Act (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296; 6 U.S.C. § 1141; 6 U.S.C. § 1161.

<sup>2</sup> Modal security plans for Aviation, Maritime, Surface, and Intermodal are described in the [2020 Biennial National Strategy for Transportation Security \(NSTS\)](#), published May 29, 2020. This report closes out the modal plans, activities, and objectives from the 2020 NSTS.

As required by law, this report is being provided to the following Members of Congress:

The Honorable Maria Cantwell  
Chair, Senate Committee on Commerce, Science, and Transportation

The Honorable Ted Cruz  
Ranking Member, Senate Committee on Commerce, Science, and Transportation

The Honorable Gary C. Peters  
Chairman, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Rand Paul  
Ranking Member, Senate Committee on Homeland Security and Governmental Affairs

The Honorable Sherrod Brown  
Chairman, Senate Committee on Banking, Housing, and Urban Affairs

The Honorable Tim Scott  
Ranking Member, Senate Committee on Banking, Housing, and Urban Affairs

The Honorable Mark E. Green  
Chairman, House Committee on Homeland Security

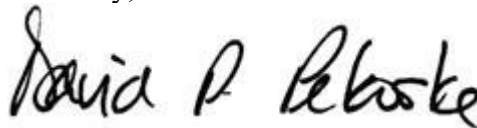
The Honorable Bennie G. Thompson  
Ranking Member, House Committee on Homeland Security

The Honorable Sam Graves  
Chairman, House Committee on Transportation and Infrastructure

The Honorable Rick Larsen  
Ranking Member, House Committee on Transportation and Infrastructure

Inquiries relating to this report may be directed to me at (571) 227-2801 or TSA's Legislative Affairs office at (571) 227-2717.

Sincerely,

A handwritten signature in black ink that reads "David P. Pekoske". The signature is written in a cursive, slightly slanted style.

David P. Pekoske  
Administrator

# Executive Summary

This “Annual Report on Transportation Security” addresses multiple reporting requirements,<sup>3</sup> through the summary of activities and accomplishments of the Transportation Systems Sector (TSS) during the FY 2022 time period, unless otherwise noted. This report provides an assessment of progress made in implementing modal security plans from the 2020 National Strategy for Transportation Security (NSTS).<sup>4</sup>

The 2020 NSTS provided the following three overarching strategic goals to guide the objectives and activities in each modal security plan.

Goal 1:	Manage risks to transportation systems from terrorist attacks and enhance system resilience.
Goal 2:	Enhance effective domain awareness of transportation systems and threats.
Goal 3:	Safeguard privacy, civil rights and civil liberties; and, the freedom of movement of people and commerce.

The TSS consists of four distinct and inter-connected modes:

- Aviation
- Maritime
- Surface
- Intermodal

Modal security plans were designed to build and enhance the resiliency of critical transportation infrastructure and assets. These plans provide a path to achieve desired outcomes. In part, outcomes specifically aimed to ensure:

- Weapons of mass destruction (WMDs) are not carried in commercial transportation.
- Chemical and biological threats are detected and neutralized.
- Information systems vital to the safe, secure, and efficient operation of transportation systems are protected from malicious cyber activity.
- Terrorists are not able to travel by commercial aviation.
- Employees in security sensitive positions are vetted to minimize risks from insider threat.
- Transportation systems and conveyances are not used as weapons (for example, bulk containers of toxic, flammable, or explosive materials).
- Exercise and training services build operational capacity through domain awareness and application of best practices.

---

<sup>3</sup> Reporting requirements are mandated by the 2001 Aviation and Transportation Security Act (Pub. L. 107-71), 2004 Intelligence Reform and Terrorism Prevention Act (Pub. L. 108-458), and 2007 Implementing Recommendation of the 9/11 Commission Act of 2007 (Pub. L. 110-53). Specific requirements are summarized in this report, within section I. Legislative Language.

<sup>4</sup> The [2020 NSTS](#) was published May, 29, 2020. The updated [Biennial NSTS](#) was published on April 18, 2023. This annual report summarizes progress on the modal plans from the 2020 strategy, unless otherwise indicated.

Section II of this report provides a summary of progress in each mode and the key accomplishments related to the goals, objectives, and activities outlined in the 2020 NSTS.

In brief, the TSS continued activities to secure and advance the resilience of our Nation's critical transportation infrastructure. In 2022, TSA marked 20 years of checkpoint federalization at more than 400 airports across the country, and passenger volumes at airports and in public transportation moved closer to pre-pandemic levels.<sup>5</sup> Although passenger volumes increased, the aftermath of the COVID-19 pandemic continued to challenge the TSS.

For industry, this meant tight fiscal constraints and limited in-person security training and participation in security programs and exercises such as the TSA Baseline Assessment for Security Enhancement (BASE) and Intermodal Security Training and Exercise Program (I-STEP). Non-regulatory assessments and security workshops and exercises evaluate the security posture of industry operations, promote preparedness, and provide an opportunity to learn and share best practices with peers and surrounding communities. When possible, industry and government engaged utilizing virtual capabilities, and a hybrid combination of physical and virtual capabilities, to connect with stakeholders and continue security awareness and cybersecurity training.

TSA, on behalf of co-SRMAs DOT and USCG, surveyed industry partners in the TSS regarding the use and adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework. TSA analyzed survey responses to better understand industry awareness and use of the framework so that co-SRMAs can help industry manage and reduce cybersecurity risks to critical infrastructure.<sup>6</sup>

TSA improved Security Directives and programs using security measures that are performance-based and outcome-focused. These security measures are more adaptable to changes in technology, process improvements, and the unique capabilities and operating environments of system owners and operators.<sup>7</sup>

In the weeks leading up to Russia's invasion of Ukraine in February 2022, TSA initiated a multifunctional Crisis Response Team to ensure leaders across TSA and the transportation industry were kept informed on the evolving conflict and potential impacts to the transportation industry.<sup>8</sup>

---

<sup>5</sup> TSA Officers screened over 736 million passengers in 2022, averaging over 2 million passengers per day. A day-to-day summary of TSA checkpoint travel numbers from 2019–2023 can be viewed on [TSA.gov](https://www.tsa.gov); the public transportation industry saw ridership rebound to more than 70 percent of pre-pandemic levels: [American Public Transportation Association \(APTA\)](https://www.aptanet.org).

<sup>6</sup> January 2023 report, NIST Cybersecurity Framework Use and Adoption in the Transportation System Sector: Survey Results and Analysis.

<sup>7</sup> In FY 2022, TSA issued two Cybersecurity Security Directives and one Information Circular for Pipelines, two Security Directives for Railroads, and three Information Circulars for other surface modes. In Aviation, TSA issued three Information Circulars and three sets of security program changes.

<sup>8</sup> In FY 2022, this Crisis Response Team provided over 100 intelligence and information sharing products at varying levels of national security classification.

TSA expanded information sharing capabilities and industry and government collaborated to nurture communication channels to enhance awareness, provide more timely information, conduct analysis, and determine potential risks.<sup>9</sup> The Charter for the Surface Information Sharing Cell (SISC) was finalized and expanded its intelligence and information sharing program.<sup>10</sup> Surface transportation industry owners and operators exchanged information with national, state, local, tribal, and territorial government partners through a variety of engagements and platforms. For example, the SISC delivered over 1,000 threat-information reports via the secure Homeland Security Information Sharing Network (HSIN).<sup>11</sup> The SISC provides a platform for coordination between government and the surface industry, similar to the Aviation Domain Intelligence Integration and Analysis Cell (ADIAC).<sup>12</sup> Both the SISC and ADIAC integrated TSA and multi-agency briefs into their daily threat briefings to support access to agency perspectives and finished intelligence products.

Enrollment in trusted traveler and vetting programs increased for almost every program.<sup>13</sup> In addition, the number of renewals completed online increased, and virtual and remote capabilities were used to maximize services.<sup>14</sup> Efficient and comprehensive vetting for the TSS mitigates potential passenger and insider threats to transportation.

---

<sup>9</sup> More information on how TSA shares information to protect against threats to transportation is provided in the Transportation Security Information Sharing Environment (TSISE) report to Congress. TSA submitted the TSISE report for FY 2022 on January 17, 2023.

<sup>10</sup> The SISC increased two-way sharing of cyber threat information products by 30 percent over FY 2021. TSA formed the SISC consistent with a recommendation of the Surface Transportation Security Advisory Committee (STSAC) to facilitate a surface transportation public-private information sharing cell. The STSAC operates under authority provided by the TSA Modernization Act (Pub. L. No. 115-254, 132 Stat. 3186, October 5, 2018). The SISC Charter was approved by officials from TSA, DOT, the Rail Sector Coordinating Council, Mass Transit Sector Coordinating Council, the Highway Motor Carrier Sector Coordinating Council, and the Pipeline Security Working Group.

<sup>11</sup> DHS communicates in real-time with its partners utilizing HSIN. Since 2015, TSA has used Info Boards on HSIN to share information with industry. This platform provides a secure repository of information used daily to facilitate a controlled exchange of Sensitive Security Information (SSI).

<sup>12</sup> The ADIAC is a flagship information sharing cell, sponsored in 2016 via ODNI National Aviation Intelligence Integration Office and approved by the DHS Chief of Intelligence.

<sup>13</sup> At the end of FY 2022, the active TSA PreCheck® application program population stood at 13.48 million. This was an increase of 26 percent from the 10.7 million at the start of FY 2022. The Transportation Worker Identification Credential (TWIC) enrollment increased 19 percent from the amount in FY 2021; TSA PreCheck® enrollment increased 128 percent from the amount in FY 2021; and the Hazardous Material Endorsement (HME) enrollment increased 3 percent from FY 2021.

<sup>14</sup> In FY 2022 online renewals accounted for 95 percent of all renewals. TSA began offering online renewal services for TWIC applicants on August 20, 2022.

TSA also expanded domestic programs such as the National Deployment Force;<sup>15</sup> deployed new checkpoint technologies to improve security effectiveness, efficiency, and the customer experience at airports nationwide;<sup>16</sup> and intercepted a record number of firearms at security checkpoints.<sup>17</sup>

---

<sup>15</sup> The National Deployment Force is comprised of 1,000 transportation security officers who are deployed in times of need, such as: staffing shortages, increased throughput volume, COVID-19 surges, and high-traffic events. In FY 2022, over 3,800 deployments provided support to 132 field locations.

<sup>16</sup> TSA deployed 534 Credential Authentication Technology (CAT) units and added 243 Computed Tomography X-ray scanners at airport checkpoints to reduce physical contact and improve security effectiveness; began software updates to on-person screening technology to enhance security and reduce the use of pat-downs; and piloted a mobile driver's license program at airports across the country (ex. Arizona, Colorado, and Maryland).

<sup>17</sup> In FY 2022, 6,542 firearms (88 percent loaded) were prevented from entering the secure areas of airports, and TSA increased the maximum civil penalty for a firearms violation to nearly \$15,000.



# FY 2022 Annual Report on Transportation Security

## Table of Contents

Message from the Administrator.....	i
Executive Summary .....	i
I. Legislative Language.....	1
II. Sector Progress .....	2
A. Aviation .....	2
B. Maritime.....	8
C. Surface .....	12
D. Intermodal.....	25
III. Looking Forward .....	28
Appendix A: Acronymns .....	30



# I. Legislative Language

This report combines multiple annual reporting requirements to streamline DHS submission of various reports on transportation security.

## **49 U.S.C. § 114(s)(4)(C)<sup>18</sup>**

In part, this requirement states: The Secretary of Homeland Security shall submit to the appropriate congressional committees an assessment of the progress made on implementing the National Strategy for Transportation Security, including the transportation modal security plans.

## **49 U.S.C. § 44938(a)<sup>19</sup>**

In part, this requirement states: The Secretary of Homeland Security shall submit to Congress a report on transportation security with recommendations the Secretary considers appropriate.

## **Section 109(b) of the Aviation and Transportation Security Act (Pub. L. No. 107-71) (49 U.S.C. § 114 note, 115 Stat 613-614), as amended by Pub. L. No. 107-296<sup>20</sup>**

In part, this requirement states: Annually until the Under Secretary has implemented or decided not to take each of the actions specified in subsection (a), the Under Secretary shall transmit to Congress a report on the progress of the Under Secretary in evaluating and taking such actions, including any legislative recommendations that the Under Secretary may have for enhancing transportation security.

## **6 U.S.C. § 1141<sup>21</sup>**

In part, this requirement states: An annual report on the national strategy for public transportation security be provided to Congress on the state of public transportation security in the United States, which shall include the status of security assessments, the progress being made around the country in developing prioritized lists of security improvements necessary to make public transportation facilities and passengers more secure, the progress being made by agencies in developing security plans and how those plans differ from the security assessments and a prioritized list of security improvements being compiled by other agencies, as well as a random sample of large- and small-scale projects currently underway.

## **6 U.S.C. § 1161<sup>22</sup>**

In part, this requirement states: An annual report shall be provided to Congress containing an assessment on the national strategy for railroad transportation security.

---

<sup>18</sup> [49 U.S.C. § 114](#)

<sup>19</sup> Ibid.

<sup>20</sup> Ibid.

<sup>21</sup> [6 U.S.C. § 1141: Reporting requirements \(house.gov\)](#)

<sup>22</sup> [6 U.S.C. § 1161: Railroad transportation security risk assessment and National Strategy \(house.gov\)](#)

## II. Sector Progress

In FY 2022, the TSS continued efforts to enhance security and resiliency in an evolving landscape. This section summarizes progress in each mode, with tables containing key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS. All information is from the FY 2022 time-period, unless otherwise indicated.<sup>23</sup>

### A. Aviation

The Aviation domain includes aviation assets and systems, such as the cyber, human, and physical elements of air cargo systems, commercial airlines and airports, general aviation, flight schools, and repair stations.<sup>24</sup>

Threats to Aviation systems include, hijackings, errant and nefarious unmanned aircraft systems, mass casualty attacks on airplanes or airports, and cyber-attacks. Air cargo comprises public and private sector stakeholders that engage in an elaborate network of commerce and security activities. This environment has increased in complexity throughout the past decade, in part, due to the rise of e-commerce and air cargo volumes. In domestic aviation operations, inspections were conducted at all regulated airports to ensure compliance with TSA regulations.

Enrollment in trusted traveler programs such as TSA PreCheck<sup>®</sup> and CBP programs—including Secure Electronic Network for Travelers Rapid Inspection (SENTRI), NEXUS, Free and Secure Trade (FAST), and Global Entry—continued to expand. Participation in these programs helps identify low-risk air travelers and provides expedited security screening at U.S. airports and when crossing international borders. TSA accepted seven new airlines into TSA PreCheck<sup>®</sup> and reduced the initial cost for enrollment from \$85 to \$78. The cost for online renewal remained \$70.

---

<sup>23</sup> The 2020 NSTS was published May, 29, 2020. The updated Biennial NSTS was published on April 18, 2023. This annual report summarizes progress on the modal plans from the 2020 strategy, unless otherwise indicated.

<sup>24</sup> Air cargo operations serving the United States are made up of over 300 domestic and foreign air carriers, and over 4,000 indirect air carriers. Commercial airlines are those that engage in regularly scheduled passenger service or public charter operations, including domestic aircraft operators and foreign air carriers flying within, from, to, or over the United States. Certain private charter operations are also deemed commercial flights. Commercial service airports are defined as public airports that have at least 2,500 passenger boarding's per year and have scheduled passenger service (Title 49 U.S.C. 47102(7)). Over 400 airports in the United States have airport security programs. General aviation is defined as aircraft operation for personal, recreational, or other noncommercial (any flights not accepting money for passenger or cargo) purposes. General aviation aircraft use approximately 19,300 private and public airports, heliports, and landing strips in the United States, of which more than 5,100 are public-use airports, including commercial airports described above. Flight schools include any pilot school, flight-training center, air-carrier flight-training facility, flight instructor, or any other person or entity that provides instruction in the operation of any aircraft or aircraft simulator. Air traffic control is a service provided by ground-based air traffic controllers who direct aircraft on the ground and through controlled airspace, and can provide advisory services to aircraft in non-controlled airspace. The primary purpose of air traffic control worldwide is to prevent collisions, organize and expedite the flow of air traffic, and provide information and other support for pilots. Foreign and domestic repair stations inspect, repair, replace, or overhaul aviation products and articles, including airframes, engines, propellers, and radios among others.

TSA remained committed to providing responsive communication to traveler’s questions and inquiries. In 2022:

- The TSA Contact Center answered 1.9 million traveler calls and emails.
- AskTSA responded directly to 2.2 million inquiries, typically within 2 minutes.
- TSA introduced a new feature for travelers to text security-related questions to AskTSA (or 275-872 on the keypad).
- Additionally, the TSA Cares helpline provided assistance to 46,000 travelers with disabilities, medical conditions, and other special needs.

International partnerships remained essential to advancing security in aviation and other modes. TSA’s efforts on international oversight, information sharing, advisory, and coordination are supported by TSA Representatives (TSARs), International Industry Representatives (IIRs), and Regional Directors (RDs). In FY 2022, in support of our international efforts, TSA:

- Participated in the United Kingdom (UK) Information Exchange with UK security partners.
- Reached an agreement with Airports Council International—Europe on piloting open architecture airport security technology.
- Opened the first international TSA PreCheck® location in the Bahamas.
- Approved Bermuda to preclear checked baggage, allowing it to reach its final destination without having to be re-screened at U.S. airports.

**Table 1** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS for Aviation.

**Table 1: Aviation NSTS Modal Security Plan Progress Assessment**

<b>Goal 1: Manage risks to the Aviation Transportation Subsector from terrorist attacks and enhance system resilience</b>
Objective 1.1: Improve physical and cybersecurity of domestic aviation critical infrastructure
Activity 1.1.1: Increase the number of aviation workers requiring a fingerprint-based criminal history records check and increase the use of Rap Back <sup>25</sup> for recurrent criminal vetting of workers requiring unescorted access to non-public areas of airports
Key Accomplishments: <ul style="list-style-type: none"> <li>• There are 326 airports and 69 aircraft operators participating in Rap Back with over 1.3 million active subscriptions out of an estimated population of 1.7 million. Active Rap Back subscriptions increased by 28 percent, gaining 301,000 subscriptions.</li> <li>• TSA revoked 704 Transportation Worker Identification Credentials (TWIC) and 1,730 Known Traveler Numbers (KTN) due to information TSA received through Rap Back.</li> </ul>
Activity 1.1.2: Assess cybersecurity vulnerabilities of commercial aircraft and airports survey
Key Accomplishments: <ul style="list-style-type: none"> <li>• TSA conducted airport cybersecurity training courses with 94 participants from 23 airports.</li> </ul>

<sup>25</sup> Rap Back is a FBI program that provides continuous vetting of a person’s suitability for his/her position of trust.

- TSA strengthened training and evaluation of radar operators by providing tactics, techniques, and procedures to better determine cyber-attacks on radar systems.
- TSA hosted four conferences to expand stakeholder awareness and demonstrate tools and resources to secure the aviation ecosystem from a cyber-attack.
- DHS transitioned the Aviation Cyber Initiative from CISA to TSA. The transition:
  - Brings the initiative under the Sector Risk Management Agency (SRMA) umbrella.
  - Uses existing partnerships to foster better collaboration between government and industry stakeholders.
  - Reduces risk and improves cyber resiliency across the aviation ecosystem.

Activity 1.1.3: Assess Unmanned Aircraft System (UAS) risk in the environs of commercial airports

Key Accomplishments:

- TSA conducts UAS assessments jointly with airport authorities to identify vulnerabilities and threats posed by nefarious and errant UAS operators and provide recommendations to mitigate those vulnerabilities to airport and local stakeholders. TSA uses the UAS assessments to refine tactical response plans, define site-specific operational plans, build response capabilities at airports, and prepare justifications for mitigation measures and technologies procurement.
- Fifteen UAS assessments were conducted at commercial airports.
- TSA created and co-chaired, with the Federal Bureau of Investigation (FBI), a working group on counter-UAS technology. This group contains 30+ member agencies (approximately 160 working group members) dedicated to the shared goal of developing standardized strategies for counter-UAS technology testing and data dissemination.

Objective 1.2: Improve capabilities to prevent, protect, mitigate, respond to, and recover from terrorist attacks throughout the aviation community

Activity 1.2.1: Strengthen technical skill of frontline employees to identify, deter, prevent, and respond to threats by expanding training and development programs and security awareness messaging describing common threat indicators

Key Accomplishments:

- TSA conducted over 760 covert tests during more than 200 airport visits. These tests used six scenarios, which included checked baggage testing. Based on the results of these tests, TSA issued four recommendations to improve security effectiveness. The four recommendations included options for improvement in the areas of checked baggage screening, pat-downs, and X-ray screening processes, including improvements needed specifically for Advanced Technology-2 X-ray screening lanes.<sup>26</sup>
- TSA trained 257 canines and deployed more than 1,000 explosives detection canine teams to airports and mass transit facilities to support large-scale events such as Super Bowl LVI, the Kentucky Derby, and Indy 500. These deployments enhanced security operations at airports and surface transportation systems nationwide. TSA partnered with CISA to train transportation security inspectors in analysis of vulnerabilities, global threat activity, and

<sup>26</sup> The recommendations based on the results of covert tests are Sensitive Security Information (SSI).

global industry trends. TSA and CWMD partnered to provide joint radiological and nuclear detection operations at these special events.

- Sixty-one TSA employees attended Embry Riddle and the International Civil Aviation Organization (ICAO) cybersecurity training. This training focused on leadership and technical skills required to develop a cybersecurity plan, conduct risk assessments, and respond to incidents.
- TSA created insider threat awareness campaigns to increase workforce knowledge of potential risk indicators and how to report potential cases.

**Objective 1.3: Enhance international aviation security risk management strategies**

**Activity 1.3.1: Conduct outreach to facilitate the use of international best practices and procedures**

**Key Accomplishments:**

- TSA provided National Inspector and International Compliance Inspector support to 13 foreign delegations.
- TSA and Mexico signed a Sensitive Security Information (SSI) sharing agreement, focused on expanding threat mitigation capabilities.
- TSA partnered with 100 percent of Last Point of Departure airports<sup>27</sup> to improve security by addressing identified vulnerabilities and gaps. Through engagement and several initiatives with foreign partners, the Agency continued to strengthen global aviation security.
- Provided technology and training to El Salvador, Philippines, Haiti, Ethiopia, Nigeria, and Somalia to mitigate vulnerabilities and improve the global transportation network.
- Coordinated with the Department of State to complete the first ever Saudi air marshal training course in Riyadh, Kingdom of Saudi Arabia.
- Finalized an agreement with Republic of Korea to conduct a Common View Air System pilot. Provided guidance and standards for 12 foreign delegations to validate international baggage and cargo security requirements.
- Finalized a Joint Declaration of Intent, signed by TSA and representatives from Germany, the Netherlands, and the UK to harmonize technical standards and establish methods to align security screening equipment standards at airports.
- Continued One Stop Security (OSS) engagement efforts between U.S. and foreign government partners, to include identifying foreign and domestic U.S. airports for evaluation and participation in the OSS pilot. The OSS pilot with London Heathrow (LHR) continued at pace, working towards pilot phase 1, for flights from the United States to the UK.
- Provided Threat Image Projection (TIP) library to Japan, Nigeria, Ireland, and the UK, to improve detection and threat recognition.

**Activity 1.3.2: Assess compliance with security measures required for service to the United States**

**Key Accomplishments:**

- TSA conducted 165 inspections of air carriers at LPD airports to ensure compliance with TSA program requirements. TSA also conducted assessments of LPD airports for adherence to

<sup>27</sup> A foreign airport from which a carrier provides direct service to the United States.

<p>ICAO standards. In addition, TSA conducted 139 assessments of LPD airports.</p> <ul style="list-style-type: none"> <li>• TSA updated its Foreign Airport Assessment Report to align with requirements in the revised ICAO standards and recommended practices, Amendment 18, effective November 18, 2022.<sup>28</sup></li> <li>• TSA provided National Inspector and International Compliance Inspector support to 13 foreign delegations.</li> <li>• TSA conducted four Regional Security Strategy (RSS) sessions to identify and mitigate vulnerabilities associated with Foreign Airport Assessments. RSS are part of the larger mitigation planning process in which TSA identifies mitigation activities to address identified vulnerabilities.</li> </ul>
<p>Activity 1.3.3: Scan international inbound air cargo shipments entering the U.S. to detect radiological or nuclear threats</p>
<p>Key Accomplishment:</p> <ul style="list-style-type: none"> <li>• CBP continues to work with CWMD and the U.S. Postal Service to streamline operations and capabilities of radiation detection systems upon entering the U.S. at a port of entry.</li> </ul>
<p>Objective 1.4: Increase security technology capability to respond to known and emerging threats</p>
<p>Activity 1.4.1: Leveraging TSA work to harmonize standards internationally and improve aviation industry stakeholder participation in the research and development process for threat detection and screening capabilities</p>
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• TSA engaged with two domestic airports (Akron, Ohio, and Houston, Texas) and 6 international airport stakeholders (Australia, Canada, Germany, Israel, New Zealand, and the United Kingdom); as well as federal, state, and local governments and academia to strengthen partnerships, communicate TSA priorities, advance technological capabilities, and drive innovation through research, outreach, and demonstration.</li> <li>• TSA engages with stakeholders from both the public and private sectors through industry day events, conferences, and speaking engagements, focusing on R&amp;D for threat detection and screening capabilities. TSA facilitated 17 panels and workshops.</li> <li>• The TSA Innovation Task Force completed the demonstration of three different capabilities: an advanced training solution, a threat detection algorithm for Computed Tomography (CT) accessible property screening, and a data infrastructure solution focusing on integrating TSA’s operational data. The information yielded from these demonstrations will advance data analysis capabilities and the cyber security of TSA equipment.</li> </ul>
<p><b>Goal 2: Enhance effective aviation domain awareness of transportation systems and threats</b></p>
<p><b>Objective 2.1: Improve quality in the sharing of intelligence information and products for government, industry, and public awareness</b></p>
<p>Activity 2.1.1: Enhance the quality and applicability of intelligence sharing with security partners</p>
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• TSA met its goal of providing intelligence information that helps customer organizations accomplish their missions and objectives. TSA improved its ability to share intelligence</li> </ul>

<sup>28</sup> <https://www.icao.int/Newsroom/Pages/Updated-Aviation-Security-standards-adopted-by-the-ICAO-Council.aspx>

information by using the Intelligence Community Production System (ICPS), modernizing information sharing platforms such as TSA’s HSIN portal, and making efforts to adopt foreign disclosure and release governance to improve dissemination capability.

- TSA Intelligence and Analysis (I&A) surveyed an additional 31 customers, yielding 25 additional survey responses. The agency observed a 4 percent increase in survey responses compared to FY 2021, and 86 percent of stakeholders said TSA I&A met their intelligence needs.
- TSA participated in over a dozen aviation security-related ICAO working groups and panels, that included participation in the ICAO annual Global Aviation Security Symposium (AVSEC).

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

**Objective 3.1: Apply risk-based security approach to supply chain and passengers**

Activity 3.1.1: Resolve security risks associated with high-risk cargo identified by the Air Cargo Advance Screening program, by screening all inbound air cargo shipments prior to loading onto aircraft destined for the United States

Key Accomplishment:

- The Air Cargo Advance Screening (ASAC) team adjudicated 126,830 international inbound cargo shipments. The ACAS program works to identify and prevent high-risk shipments, prior to cargo being loaded onboard flights destined to the United States.

Activity 3.1.2: Provide expedited aviation security screening for trusted travelers

Key Accomplishments:

- Trusted Traveler enrollment is very strong, with enrollment in TSA PreCheck® outpacing the pre-pandemic 2019 volume. With a higher volume of trusted travelers enrolled, plus a return to pre-pandemic travel behaviors, the percentage of travelers with a KTN exceeded program expectations.
- Over five million TSA PreCheck® customers and approximately 636,000 TWIC applicants are subscribed in Rap Back.
- Over ninety-nine percent of all passengers waited less than 30 minutes at airport security checkpoints, while 99.4 percent of passengers in TSA PreCheck® lanes waited less than 10 minutes.
- TSA Secure Flight prescreened 915 million reservations, with 1.4 million manual reviews against the Terrorist Screening Dataset (TSDS). Additionally, on a recurring basis, TSA vetted over 30 million credentials, with 525,000 manual reviews against the TSDS.
- Global Entry, a CBP program, continued to allow pre-approved, low-risk U.S. citizens and lawful permanent residents expedited clearance upon arrival into the United States. Participants enter using automated self-service kiosks and receive “front of the line” privileges.
- CBP received 3.78 million applications and enrolled 2.65 million new and renewing members into one of the four Trusted Traveler programs: Global Entry, NEXUS, SENTRI, or FAST. More than 10.5 million members enjoyed the benefits of expedited processing as

a Trusted Traveler. Overall membership for CBP’s Trusted Traveler programs grew by 8 percent.

- CBP Preclearance strategically places over 600 CBP officers and employees across 15 international locations to process passengers and their goods through customs, immigration and agricultural inspections—skipping a need for inspections upon arrival in the United States. This creates opportunities for increased security, economic growth, and an improved passenger experience.

## B. Maritime

Security of the Maritime Transportation System (MTS) is led by the USCG. The MTS encompasses a geographically, physically, and operationally diverse network of maritime and shore side operations that supports trillions of dollars of economic activity. Passengers move by ferry and cruise ships, which connect consumers, producers, manufacturers, and farmers to domestic and global markets. In the United States there are 25,000 miles of navigable channels, 250 locks, 3,500 marine terminals, and 361 ports.

Waterways by nature, are less restricted and accessible without many of the mechanisms for detection and investigation that are available in air and land domains. Security vulnerabilities come from a variety of hazards including physical and cyber-attacks. A terrorist attack in the MTS—particularly in heavily populated port areas involving hazardous cargo—could have devastating effects, adverse economic impacts, and disrupt domestic and international trade.

**Table 2** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS for Maritime.

**Table 2: Maritime NSTS Modal Security Plan Progress Assessment**

<b>Goal 1: Manage risks to transportation systems from terrorist attack and enhance system resilience</b>
Objective 1.11: Use risk-based security planning and operations to reduce the terrorism risk to the Marine Transportation System
Activity 1.1.1: Improve compliance at Maritime Transportation Security agency-regulated facilities through risk-based adjustments of enforcement operations tempo
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• Ensured all MTSA regulated facilities complied with the requirement to include cybersecurity in their Facility Security Assessment (FSA) &amp; Facility Security Plan (FSP) by October 1, 2022.</li> <li>• The Coast Guard works collaboratively with TSA, other agencies, and industry partners to identify and mitigate risk and potential threats to MTSA regulated facilities and also areas of concern within an Area Maritime Security Committee’s oversight within the MTS.</li> <li>• The Transportation Worker Identification Card (TWIC) is required for access to MTSA</li> </ul>



facilities. The TWIC program is jointly managed between TSA (responsible for enrollments, security threat assessments, credential production, and systems operations) and the U.S. Coast Guard (responsible for establishing and enforcing access control requirements for MTSA-regulated vessels and facilities). A Coast Guard Investigator is currently on assignment with TSA in support of shared TWIC equities for the agencies.

- Annually, the Coast Guard conducts risk-based assessments within ports, to include MTSA regulated facilities, and mitigates potential risk increases through amendments to the Area Maritime Security Plan.
- The Coast Guard also assesses regulatory framework, policy, and guidance to ensure their adequacy in protecting applicable entities from threats.

Activity 1.1.2: Improve interoperability of federal and state, local, tribal, and territorial (SLTT) response teams in Maritime and Security Response Operations (MSRO)

Key Accomplishment:

- FY 2022 MSRO performance efficiency exceeded the target by 6 percent. This was achieved by successful execution of Risk Based MSRO activity plans, which help field units effectively allocate resources and perform optimal risk-reducing MSRO activities. The Coast Guard's MSRO performance metric for efficiency takes into account maritime security activities performed by other federal, state, local, tribal, and territorial government agencies in support of Coast Guard missions.

Activity 1.1.3: Employ Maritime Security Risk Analysis Model (MSRAM)<sup>29</sup> and other risk assessments and analysis tools to refine the estimates of MSRO activities' risk-reduction benefits, and use these estimates to inform the execution of MSRO activities in U.S. ports

Key Accomplishment:

- Coast Guard metrics revealed Operational Commanders are utilizing available resources at efficiency rates above annual targets. This indicates the Coast Guard is getting the most risk reduction value out of its available resources. Competing mission demands and resource constraints are currently limiting risk reduction target achievement.

Activity 1.1.4: Identify and assess high-risk inbound cargo

Key Accomplishments:

- Class 7 Radioactive and Class 1 Explosives, and other similar cargos with related hazards are monitored. These include materials that may be spontaneously combustible, flammable gases, etc., with the potential to inflict significant damage to people, property and the environment.
- Inspected, and collaborated on potential enforcement action of high-risk inbound cargo.
- Multi-Agency Strike Force Operations (MASFOs) at each port involving TSA, CWMD, Pipeline and Hazardous Materials Safety Administration (PHMSA), Federal Motor

<sup>29</sup> MSRAM is a process and model that supports the USCG's mission to understand and mitigate the risk of terrorist attacks on targets in U.S. ports and waterways.

Carrier Safety Administration (FMCSA), Federal Railroad Administration (FRA), FAA, CBP, APHIS, IRS, FBI, the National Container Bureau, state, and local officials on an annual basis address joint equities of high-risk inbound cargo on collaborative and industry training scenarios.

**Objective 1.2: Reduce security vulnerabilities and improve preparedness throughout the Marine Transportation System**

Activity 1.2.1: Assess International Ship and Port Security (ISPS) Code implementation in foreign ports to receive ships destined for the United States

**Key Accomplishment:**

- Completed 80 percent of triennial port security assessments of U.S. trade partners.

Activity 1.2.2: Evaluate containerized cargo for illicit radiological or nuclear material

**Key Accomplishments:**

- Coast Guard organizes port level MASFOs, where a surge of joint inspection action involving multiple agencies with varying jurisdictions, authorities and resources collaborate to inspect a high number of containers in a small window, to increase safety, security and identify and mitigate vulnerabilities which have high potential to identify illicit radiological or nuclear material.
- USCG and TSA collaborate with the CBP on its Non-Intrusive Inspection (NII) technology enabling detection of contraband (e.g., narcotics and weapons) and materials that pose potential nuclear and radiological threats. CWMD works in conjunction with USCG, TSA, and CBP by providing additional radiological and nuclear detection equipment and personnel. Technologies deployed to our Nation’s land, sea, and air ports of entry include large-scale X-ray and Gamma ray imaging systems, as well as a variety of portable and handheld technologies. NII technologies and CWMD equipment are viewed as force multipliers that enable screenings and examinations of a larger portion of the stream of commercial traffic while facilitating the flow of legitimate trade, cargo, and passengers.

**Goal 2: Enhance effective domain awareness of MTS and threats**

Objective 2.1: Improve the security, resilience, and regulatory (federal, state, local, tribal, and territorial) information sharing process throughout the Marine Transportation System community

Activity 2.1.1: Enhance resilience of cyber systems through implementation of the National Cyber Strategy Implementation Plan, exercises, guidance, assessments, and expansion of cyber intrusion detection and remediation technology

**Key Accomplishments:**

- Enclosure 5 of Navigation and Vessel Inspection Circular (NVIC) 09-02 CH6 titled, Cyber Risk Plan Annex, has further implemented IAW Activity 2. Under NVIC 09-02 Guidelines for the Area Maritime Security Committees and Area Maritime Security

Plans required for U.S. ports, cyber is assessed, mitigation strategies are included, job aids to assist are provided.

- The Maritime Cyber Readiness Branch (MCRB) and local Coast Guard units investigated 42 cybersecurity reports in FY 2022 (including phishing/spoofing, ransomware attacks, other cyber incidents).
- The Coast Guard Cyber Protection Teams (CPTs) deployed on 23 missions in FY 2022 in support of Coast Guard Operational Commanders and organizations in the Marine Environment (including assessments, hunts, and incident response).
- Ensured all MTSA regulated facilities complied with the requirement to include cybersecurity in their Facility Security Assessment (FSA) & Facility Security Plan (FSP) by October 1, 2022.

Activity 2.1.2: Participate in and materially support the development of a national Maritime Domain Awareness tool as defined in the Maritime SAFE Act

Key Accomplishment:

- The USCG has chosen SeaVision as the relevant MDA tool of choice to achieve requirements for M-SAFE and other USCG and national strategy to provide unclassified MDA to account holders. SeaVision is a U.S. Navy program of record, and is the current tool offered to U.S. partners globally. It is a web-based maritime situational awareness tool that enables users to view and share a broad array of maritime information through several data feeds, layers, and analysis capabilities for vessel monitoring, c-IUUF, and unusual maritime activity, among other features.

Objective 2.2: Improve Maritime Transportation System stakeholder participation in the risk management process for security and resilience prioritization and programming

Activity 2.2.1: Improve effectiveness of port exercise programs by designing exercise objectives and events based on analysis of MSRAM risk data

Key Accomplishments:

The Area Maritime Security Training and Exercise Program (AMSTEP) annual requirements are listed in Enclosure 4 of NVIC 09-02 (series). Each Area Maritime Security Plan (AMSP) requires that the top three transportation security incident scenarios identified from the annual validation of MSRAM to be exercised within a four-year exercise cycle. The objectives are formulated around these scenarios. The exercises may be discussion based (e.g., tabletop exercise (TTX), workshop, etc.), or operational based (e.g., Functional Exercise (FE) or a Full Scale Exercise (FSE)). AMSTEPS also identify and validate the security procedures for critical infrastructure within the port. An after-action report is required, and best practices/lessons learned are shared. Corrective Action items are implemented when a process or section of the plan identifies gaps that need to be addressed. Improvements are also updated in the NVIC to improve the effectiveness of this exercise program.

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

Objective 3.1: Collaborate with international partners to increase the reliability of the global

supply chain
Activity 3.1.1: Apply risk segmentation methods to evaluate cargo for expeditious clearance
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• The USCG, within the last year,<sup>30</sup> began staffing the DHS Supply Chain Resiliency Center with an aim to preserve the US supply chain from identified risks. Preserving the global supply chain by its efforts.</li> <li>• The USCG and CBP sends a State Department approved delegation to the International Maritime Organization (IMO), Maritime Commerce Facilitation Committee (FAL), to discuss issues with regard to human and wildlife trafficking, as well as trade disruptions for legitimate radioactive cargos, among other issues.</li> </ul>

## C. Surface

Surface transportation is vast and includes mass transit and passenger rail, freight rail, highway and motor carrier, and pipelines.<sup>31</sup> These modes primarily operate within open-architecture and provide essential services to efficiently move people and goods in both domestic and international markets. Threats include mass-casualty attacks, sabotage, chemical attacks, cyber-attacks, vehicle ramming, and impacts from increased demands on aging infrastructure and natural disasters. To remain effective despite these many challenges, industry owners and operators in concert with the Federal Government and state, local, tribal, and territorial governments continually engage to reduce risks. This is accomplished in part, by the exchanging of information, researching, participation participating in exercises and assessments, planning, and training. TSA maintains oversight through regulations and security directives focused on higher risk operations.<sup>32</sup>

TSA approved 135 security training programs from surface transportation owners and operators, which is 93 percent of the total programs TSA anticipated receiving based on requirements.<sup>33</sup> Of the 135 approvals, 26 are from Freight Rail entities, 48 are from Public Transit and Passenger Rail entities, and 61 are from Over-the-Road Bus (OTRB) entities.

<sup>30</sup> As of May 8, 2024.

<sup>31</sup> Mass transit and passenger rail includes transit buses, trolleys, monorails, heavy rail (subway), light rail, streetcars, and commuter and intercity passenger railroads. Approximately 6,800 local transit providers served more than 34 million daily riders and nearly 6.2 billion unlinked passenger trips in 2022. See: <https://www.apta.com>. Amtrak and Alaska Railroad provide the Nation’s only long-distance passenger rail. Amtrak carried approximately 22.9 million passengers in FY 2022. See: <https://www.amtrak.com>. Freight rail includes over 138,000 miles of railroad track, and over 500 individual railroads. Highway and motor carrier includes over 600,000 bridges, hundreds of roadway tunnels, and over a million trucking companies with millions of trucks. School buses and motor coach companies are also included in this domain. Approximately 500,000 school buses transport nearly 25 million students each day throughout the United States. The pipeline mode has more than 3.3 million miles of regulated pipeline in the U.S. network, transporting a majority of the natural gas and hazardous liquids, including crude and refined petroleum. Above ground pipeline assets include compressor stations, pumping stations, and liquefied natural gas (LNG) facilities.

<sup>32</sup> TSA Security Directives can be found on [TSA.gov](https://www.tsa.gov).

<sup>33</sup> TSA requirements for security training plans are provided in 49 CFR parts 1580 (Freight Rail), 1582 (Mass Transit and Passenger Rail) and 1584 (Over-the-Road Bus).

TSA conducted a tabletop exercise with approximately 400 participants that included freight rail and pipeline operators and other federal partners. The Agency conducted this exercise to review readiness to communicate and coordinate with each other during a scenario involving an escalating cyber-threat. Another series of tabletop exercises included public transportation, school buses, and OTRBs in Maryland, New Jersey, and California.

TSA used the voluntary BASE program to evaluate in-place security programs, training, and the overall security posture of public transportation agencies, school buses, motor-coach, and trucking operations. BASE evaluates the security posture of an entity’s operation against multiple security action items, including security planning, training, exercise programs, and other areas important for a comprehensive security program.

TSA collaborated with Amtrak to complete two 90-day passenger vetting assessments between December 2021 and October 2023. The first vetting assessment was conducted over a 90-day period from December 2021 to March 2022 within Amtrak’s North East Corridor for passengers whose travel included stops between Washington, D.C., and New York City. The second vetting assessment was conducted over a 90-day period from July 2023 to October 2023 within Amtrak’s Inter City Passenger Route for passengers on select “long distance” travel routes originating or terminating in Chicago. A total of 1,444,500 passengers that had pre-purchased tickets via Amtrak’s online reservation system were included in the two passenger vetting assessments.

**Table 3** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS for Mass Transit and Passenger Rail.

**Table 3: Mass Transit and Passenger Rail (MTPR) NSTS Modal Security Plan Progress Assessment**

<b>Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience</b>
Objective 1.1: Security Planning: Reduce the risks associated with a terrorist attack on MTPR systems through security plans that address cybersecurity and critical infrastructure protection, and operational practices (to detect and deter)
Activity 1.1.1: Develop, review, and update security plans based on available information
Key Accomplishment: MTPR had 75 participants in the BASE with 5 of these in the high-risk category. Eighty percent of participants achieved a positive rating for security planning. <sup>34</sup> During the BASE, security plans developed by participating entities are reviewed by TSA, recommendation for improvement are discussed, and security plans are re-evaluated once updated, if necessary.
Activity 1.1.2: Develop a comprehensive cybersecurity strategy

<sup>34</sup> The BASE evaluates against several Security Actions Items (SAIs). A positive rating constitutes a combined total score of 70 percent or higher.

**Key Accomplishments:**

- TSA issued Security Directives<sup>35</sup> requiring higher risk rail and rail transit operators to have an up-to-date Cybersecurity Incident Response Plan in place for critical cyber systems. Plans must include security measures to reduce operational disruption, or other significant business or functional degradation, should their system or facility experience a cybersecurity incident. Security measures are meant to close gaps focusing on penetration testing, access controls, multi-factor authentication, encryption, network segmentation, anti-virus and anti-malware protection, and patching. All applicable owners and operators have complied with the directive.
- TSA issued Information Circulars (ICs) with cybersecurity recommendations to public transportation agencies, over-the-road buses, and other transit stakeholders not within the applicability of the Security Directives.<sup>36</sup>

**Objective 1.2: Security Training: Conduct training of employees to identify, prevent, respond, and recover from a terrorist attack**

**Activity 1.2.1: Improve the current state of the Nation's most critical MTPR systems security training programs through the incorporation of best practices and lessons learned into existing training plans**

**Key Accomplishments:**

- MTPR had 75 participants in the BASE with 5 of these in the high-risk category. Sixty-seven percent of participants achieved a positive rating for security training.
- Agencies regulated by the TSA Security Training Rule must submit a security training program to TSA for approval. In part, the plans must describe how covered owners and operators will train security-sensitive employees to observe, assess, and respond to suspected terrorist-related threats or incidents. Forty-nine MTPR agencies were required to submit training programs to TSA for approval, and at the conclusion of FY 2022, 48 training plans were approved.
- TSA offers no-cost security training materials to support owners and operators in providing “observe, assess, and respond” training for Mass Transit Bus, Mass Transit Rail, and Passenger Rail security sensitive employees.<sup>37</sup>

**Objective 1.3: Security Exercises: Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency**

**Activity 1.3.1: MTPR systems participate in exercises to evaluate the preparedness for, response to, and recovery from physical and cybersecurity incidents**

**Key Accomplishments:**

<sup>35</sup> TSA Security Directives: SD-1580-2021-01/SD-1582-2021-01 originally issued December 2, 2021 and updated October 18, 2022 (SD-1580-2021-01-A/SD-1582-2021-A); SD 1580/82-2022-01, issued October 18, 2022.

<sup>36</sup> TSA Information Circular: IC-Surface-2021-01, issued December 2, 2021; IC-Surface-2022-01, issued February 25, 2022; and IC-Surface-2022-02, issued March 23, 2022.

<sup>37</sup> TSA developed videos that cover a portion of the “Observe, Assess and Respond (OAR)” elements under 49 CFR 1580.115, 1582.115, and 1584.115.

- MTPR had 75 participants in the BASE with 5 of these in the high-risk category; 77 percent of participants achieved a positive rating for security exercises.
- As previously noted with security training, conducting exercises can be challenging due to tight fiscal constraints limiting overtime, backfill, or other funds necessary to conduct exercises.

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

Objective 2.1: Intelligence and Information Sharing: Maintain and enhance mechanisms for information and intelligence sharing between the MTPR industry and government

Activity 2.1.1: Provide timely and relevant information and intelligence to enhance industry's domain awareness

### Key Accomplishments:

- TSA provided 58 intelligence and information sharing products to mass transit and passenger rail, freight rail, highway and motor carrier, and pipeline stakeholders. TSA shared each product within 24 hours of release to keep industry informed about potential threats to transportation systems. TSA, CISA, the FBI, and other sources produced intelligence products, such as advisories and information relating to potential vulnerabilities.
- TSA participated in monthly conference calls with the Transit Security Peer Advisory Group and the broader transit community to provide intelligence updates and share best practices.
- TSA supports the Public Transportation - Information Sharing and Analysis Center (PT-ISAC) and the Over-the-Road-Bus Information Sharing and Analysis Center (OTRB-ISAC). These centers provide daily intelligence updates to industry and situational awareness messages across the sector.
- TSA facilitated quarterly MTPR Government Coordinating Council (GCC) meetings in coordination with the MTPR Sector Coordinating Council (SCC) to share information and ensure alignment with ongoing security efforts.
- TSA participated in quarterly RAILPOL Counter Terrorism Working group meetings to share best practices, intelligence, and discuss security concerns. RAILPOL (RAILway POLice) is a European association of government-controlled police organizations, with the goal to enhance and intensify international railway police cooperation, prevent threats, and link the police and the railway sector.<sup>38</sup>

Objective 2.2: Community outreach: Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with MTPR systems

Activity 2.2.1: Promote MTPR security awareness in communities surrounding critical MTPR assets and systems

### Key Accomplishment:

- Seventy-six percent of transit agencies participating in the TSA BASE program received

<sup>38</sup> <https://www.railpol.eu/site/home>

a positive rating for public awareness and emergency preparedness. This score is consistent with scores going back to FY 2017. Following a BASE assessment, TSA provides recommendations for improvement and re-evaluates participants on areas that did not have a positive rating. Owners and operators participating in the BASE program are typically evaluated on a revolving 3-year cycle.

**Table 4** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS for Freight Rail.

**Table 4: Freight Rail (FR) Progress Assessment**

<b>Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience</b>
Objective 1.1: Security Planning: Reduce the risks associated with terrorist attacks on freight railroads through security plans that address cybersecurity and critical infrastructure protection, and operational practices (to detect and deter)
Activity 1.1.1: Develop, review, and update security plans based on available information
Key Accomplishments: <ul style="list-style-type: none"> <li>TSA issued Rail Security Directive: 1580-2021-01 requiring higher-risk railroads to mitigate cyber threats to their rail transportation systems.<sup>39</sup> TSA conducted 58 inspections of owners and operators within the applicability of this Security Directive.</li> <li>One-hundred percent of railroads that transport Rail Security Sensitive Materials (RSSM) in High Threat Urban Area (HTUAs) have implemented security plans.</li> </ul>
Activity 1.1.2: Develop a comprehensive cybersecurity strategy
Key Accomplishments: <ul style="list-style-type: none"> <li>One-hundred percent of railroads that transport RSSM in HTUAs have implemented a cybersecurity strategy.</li> <li>TSA issued Security Directives<sup>40</sup> requiring owners and operators of higher-risk railroads to have an up-to-date Cybersecurity Incident Response Plan in place for critical cyber systems.</li> <li>TSA issued ICs with cybersecurity recommendations to railroads and other modes not within the applicability of the Security Directives.<sup>41</sup></li> </ul>
Objective 1.2: Security Training: Conduct training of frontline employees to identify, prevent,

<sup>39</sup> TSA SD-1580-2021-01 was issued December 2, 2021 and replaced by SD-180-2021-01-A, issued October 18, 2022.

<sup>40</sup> TSA Security Directives: SD-1580-2021-01/SD-1582-2021-01 originally issued December 2, 2021 and updated October 18, 2022 (SD-1580-2021-01-A/SD-1582-2021-A); SD 1580/82-2022-01, issued October 18, 2022.

<sup>41</sup> TSA Information Circular: IC-Surface-2021-01, issued December 2, 2021; IC-Surface-2022-01, issued February 25, 2022; and IC-Surface-2022-02, issued March 23, 2022.



and respond to a terrorist attack
Activity 1.2.1: Improve freight railroad security training programs through the incorporation of best practices and lessons learned in existing training curriculum
<p>Key Accomplishment:</p> <ul style="list-style-type: none"> <li>• One-hundred percent of railroad employees that transport RSSM in HTUAs have received security-related training during the reporting period.<sup>42</sup></li> <li>• TSA conducted several cybersecurity focused workshops with freight rail participation in Massachusetts, Arizona, Michigan, Mississippi, Louisiana, and Ohio.</li> </ul>
Objective 1.3: Security Exercises: Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency
Activity 1.3.1: Railroads participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents
<p>Key Accomplishment:</p> <ul style="list-style-type: none"> <li>• TSA conducted 15 security exercises and workshops with participation from freight rail operators, to prevent and respond to evolving security threats.</li> </ul>
<b>Goal 2: Enhance effective domain awareness of transportation systems and threats</b>
Objective 2.1: Intelligence and Information Sharing: Maintain and enhance mechanisms for information and intelligence sharing between the freight rail industry and government
Activity 2.1.1: Provide timely and relevant information and intelligence to enhance freight railroads' domain awareness
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• TSA participated in an American Association of Railroads (AAR) Rail Information Security Committee (RISC) conference calls and broader industry calls. These meetings provided an opportunity to exchange ideas and information with cyber-security and information-security representatives of the Class I railroads.<sup>43</sup></li> <li>• TSA provided 58 intelligence and information sharing products to mass transit and passenger rail, freight rail, highway and motor carrier, and pipeline stakeholders. TSA shared each product within 24 hours of release to keep industry informed about potential threats to transportation systems. TSA, CISA, the FBI, and other official intelligence and information sources produced intelligence products, such as advisories and information relating to potential vulnerabilities.</li> </ul>
Objective 2.2: Community Outreach: Engage with first responders and the public to provide awareness of security concerns associated with railroad operations in order to promote

<sup>42</sup> The TSA Security Training Rule requires that covered railroads provide security awareness training to all of their security-sensitive employees. This training ensures a baseline level of awareness and the best practices for observing, assessing, and responding to potential security threats.

<sup>43</sup> Reported by the American Association of Railroads, Class I railroads have revenues of at least \$900 million. <https://www.aar.org/facts-figures>. Accessed April 10, 2024.

situational security awareness and preparedness
Activity 2.2.1: Promote freight railroad security awareness in communities surrounding critical freight assets and systems
<p>Key Accomplishment:</p> <ul style="list-style-type: none"> <li>Railroads that transport RSSM in HTUAs reported continued engagements and activities with public safety, law enforcement, or emergency preparedness organizations.</li> </ul>

**Table 5** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS for Highway and Motor Carrier.

**Table 5: Highway and Motor Carrier (HMC) NSTS Modal Security Plan Progress Assessment**

<b>Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience</b>
Objective 1.1: Security Planning: Reduce the risks from a terrorist attack on HMC systems through security plans that address cybersecurity and critical infrastructure protection, and operational practices (to detect and deter)
Activity 1.1.1: Develop, review, and update security plans based on available information
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>TSA conducted 102 BASE assessments within HMC (52 school bus companies; 41 school districts; 5 OTRB; 4 trucking). These assessments provide a random sample of operators’ non-regulatory implementation of recommended security measures, and identify progress and areas needing improvement. Due to this mode’s large number of operators, TSA prioritized assessments of operations within HTUAs.</li> <li>TSA continued a re-visitation plan with HMC stakeholders who participated in the BASE program. Follow-up with participants supports their continued improvement and security posture.</li> <li>TSA conducted 15 Security Enhancement Through Assessment (SETA) events with HMC stakeholders. This non-regulatory and collaborative assessment is designed to evaluate and improve a stakeholder’s security posture of front-line employees through a three-phase approach of initial assessment, training, and reassessment. These tactical-level assessment scenarios included vehicle inspection procedures, unattended bag response, and other tailored assessments based on stakeholder input.</li> </ul>
Activity 1.1.2: Develop a comprehensive cybersecurity strategy
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>One-hundred-four HMC operators participated in BASE, with one operation in the high-risk category.</li> <li>A working group convened to refine cybersecurity related Security Action Items (SAIs) for incorporation into the BASE program for implementation in FY 2023.</li> </ul>

- TSA issued ICs<sup>44</sup> with cybersecurity recommendations to OTRB and other modes. Cybersecurity recommendations included: designating a Cybersecurity Coordinator, conducting self-assessments, developing plans, and reporting incidents.
- TSA continues engagements with trucking industry partners focused on advancing cybersecurity training and resources.

Objective 1.2: Security Training: Conduct training of employees to identify, prevent, respond to, and recover from a terrorist attack

Activity 1.2.1: Improve the current state of the most critical motor carriers' security training programs through the incorporation of best practices and lessons learned into existing training plans

Key Accomplishments:

- TSA conducted a weekly review panel to ensure all security training plan submissions for OTRB and other entities covered by the TSA Security Training Rule<sup>45</sup> are compliant. TSA reviewed and approved all security training plans submitted by OTRB owners and operators.
- TSA mitigated current threats and vulnerabilities using Risk Mitigation Activities for Surface Transportation (RMAST), which typically include TSA Transportation Security Inspectors – Surface, discussing security awareness issues with stakeholders and personnel.

Objective 1.3: Security Exercises: Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency

Activity 1.3.1: Motor carriers participate in exercises to evaluate the preparedness for, response to, and recovery from security incidents

Key Accomplishments:

- TSA conducted a tabletop exercise with the American Trucking Associations. The purpose was to provide the association and their members the opportunity to review operational and security procedures that guide sharing information, implementing physical protective measures, and coordinating operations among industry employees, industry partners, and security stakeholders in the event of a security incident to HMC.
- TSA continued a plan to revisit HMC stakeholders who participated in the BASE program. Follow-up with participants supports their continued improvement and security posture.
- TSA completed 24 I-STEP and 6 Exercise Information System (EXIS) activities. These activities were based on overarching TSA risk mitigation and resilience strategies and plans, supported the identification and sharing of best practices, and improved coordination between the HMC stakeholders and local emergency responders. While the outcome of these activities was successful, the COVID-19 pandemic reduced the

<sup>44</sup> TSA Information Circulars: IC-Surface 2021-01, issued December 2, 2021; and IC-Surface 2022-01, issued February 25, 2022.

<sup>45</sup> TSA requirements for security training plans are provided in 49 CFR parts 1580 (Freight Rail), 1582 (Mass Transit and Passenger Rail) and 1584 (Over-the-Road Bus).

number of in-person exercises that we were able to complete during the first half of FY 2022.

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

Objective 2.1: Intelligence and Information Sharing: Maintain and enhance mechanisms for information and intelligence sharing between the HMC industry and government

Activity 2.1.1: Provide timely and relevant information and intelligence to enhance industry's domain awareness

Key Accomplishments:

- TSA provided 58 intelligence and information sharing products to mass transit and passenger rail, freight rail, highway and motor carrier, and pipeline stakeholders. TSA shared each product within 24 hours of release to keep industry informed about potential threats to transportation systems. TSA, CISA, the FBI, and other sources produced intelligence products, such as advisories and information relating to potential vulnerabilities.
- TSA routinely distributed CISA cybersecurity bulletins to HMC stakeholders.
- TSA helped coordinated quarterly HMC GCC meetings with the HMC SCC to discuss initiatives, share information, and ensure alignment with ongoing security efforts. TSA also facilitated joint transportation GCC and SCC meetings and provided additional opportunities for coordination and collaboration on security efforts and initiatives.

Objective 2.2: Community Outreach: Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with HMC systems

Activity 2.2.1: Promote HMC security awareness in communities surrounding critical HMC assets

Key Accomplishments:

- Seventy-six percent of high-risk OTRB companies that completed a BASE achieved a positive rating for this performance measurement. It is typical to see a yearly fluctuation in final result percentages as TSA conducts BASE assessments on a 3-year rolling basis, with a new set of stakeholders assessed each year.
- TSA conducted national-level engagements with HMC associations and their membership ensuring security awareness in communities across the United States where HMC assets operate.
- TSA conducted monthly security conference calls with three respective industry groups and the broader industry as appropriate. These meetings provide an opportunity to exchange ideas and information with cybersecurity and infrastructure security representatives throughout HMC, including trucking, school buses, and OTRB.
- Regional Security Directors conducted quarterly meetings with stakeholders in their areas of responsibility, to include HMC owners and operators and other Transportation Sector partners.

**Table 6** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS for Pipeline.

**Table 6: Pipeline NSTS Modal Security Plan Progress Assessment**

<b>Goal 1: Manage risks to transportation systems from terrorist attacks and enhance system resilience</b>
Objective 1.1: Security Planning: Reduce the risks from a terrorist attack on pipeline systems through security plans addressing critical infrastructure protection, operational practices (to detect and deter), and cybersecurity
Activity 1.1.1: Review, implement, and update security plans based on risk and guidance in the TSA Pipeline Security Guidelines
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• TSA conducted on-site reviews of security plans at 22 critical pipeline companies to assess their adherence to the security plan guidance in the TSA Pipeline Security Guidelines.<sup>46</sup></li> <li>• The guidelines are used as the standard for TSA's Pipeline Security Program Corporate Security Reviews (CSRs) and Critical Facility Security Reviews (CFSRs). In April 2021, TSA added section 7, "Pipeline Cyber Asset Security Measures", that provided recommendations on pipeline cyber asset identification; security measures for pipeline cyber assets; and cyber security planning and implementation guidance.</li> <li>• Seventy-one percent of pipeline companies participating in a CSR had security plans meeting the elements in the TSA Pipeline Security Guidelines.</li> </ul>
Activity 1.1.2: Review, implement, and update cybersecurity plans based on risk and guidance in the TSA Pipeline Security Guidelines
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• Because TSA issued Security Directives in FY 2022, cybersecurity plans were not evaluated as part of the CSR process. <ul style="list-style-type: none"> <li>○ TSA issued Security Directive Pipeline-2021-02B in December 2021, and required covered pipeline owners and operators to submit action plans and implement certain cybersecurity measures. All operators covered by this Security Directive were compliant.</li> </ul> </li> </ul> <p>TSA issued Security Directive Pipeline-2021-02C in July 2022, and replaced the previous Security Directive in this series. This Security Directive required all covered pipeline owners and operators to submit a Cybersecurity Implementation Plan (CIP) by October 25, 2023, to TSA for approval.</p>
Objective 1.2: Security Training: Conduct training of employees to identify, prevent, absorb,

<sup>46</sup> TSA first developed Pipeline Security Guidelines in 2010. This guidance was updated again in 2011, 2018, and 2021. The current version is accessible on [TSA.gov](https://www.tsa.gov). Development included collaboration with industry and government partners to develop a range of recommended security measures covering different aspects of pipeline operations.

respond to, and recover from a terrorist attack

Activity 1.2.1: Review and implement security training programs based on training requirements and guidance in the TSA Pipeline Security Guidelines

Key Accomplishment:

- Conducted on-site reviews of security plans at 22 critical pipeline companies to assess their adherence to the security plan guidance on personnel security training in the TSA Pipeline Security Guidelines with an overall implementation rate of 94 percent.

Objective 1.3: Security Exercises: Conduct exercises employing threat scenarios to evaluate and identify opportunities to improve security preparedness and resiliency

Activity 1.3.1: Pipeline systems participate in exercises to evaluate the preparedness for, response to, and recovery from physical or cybersecurity incidents

Key Accomplishments:

- Conducted on-site reviews of security plans at 22 critical pipeline companies to assess their adherence to the security plan guidance on exercises and training in the TSA Pipeline Security Guidelines.
- Sixty-three percent of pipeline companies participating in a CSR met the elements in the TSA Pipeline Security Guidelines for exercises.
- TSA participated in 5 pipeline exercises. Major exercises included the Canadian Energy Command Exercise, and the Natural Gas Exercise (NGX). The NGX, was a nationwide tabletop drill hosted by the American Gas Association (AGA), that focused on natural gas distribution and transmission cybersecurity, physical security and business continuity. The Department of Energy also participated.

Objective 1.4: Physical Security Measures: Reduce the risks from an attack on pipeline systems through physical security measures addressing critical infrastructure protection.

Activity 1.4.1: Review, implement, and update physical security measures based on risk and guidance in the TSA Pipeline Security Guidelines

Key Accomplishments:

- Conducted on-site reviews of security plans at 22 critical pipeline companies to assess their adherence to the security plan guidance on physical security and access control measures in the TSA Pipeline Security Guidelines.
- TSA determined 71 percent of pipeline companies participating in a CSR met the elements in the TSA Pipeline Security Guidelines for physical security and access control.
- In April 2021, TSA published Change 1 to the TSA Pipeline Security Guidelines and encouraged pipeline operators to identify and update their list of critical facilities according to the new criteria. This resulted in a significant increase in the number of reported critical facilities with an additional 50 operators reporting critical facilities.

Objective 1.5: Cybersecurity: Reduce the risks from a cyber-attack on pipeline systems through security measures addressing critical infrastructure protection

Activity 1.5.1: Review, implement, and update cybersecurity measures based on risk and

## guidance in the TSA Pipeline Security Guidelines

### Key Accomplishments:

- TSA issued a series of Security Directives to identified critical pipelines and ICs for non-critical pipelines to reduce risks associated with cyber-attacks.
  - The Security Pipeline-2021-01 series requires the appointment of a cybersecurity coordinator, reporting of cybersecurity incidents, and conduct of a cyber-vulnerability assessment.
  - The Security Directive Pipeline-2021-02 series requires cybersecurity mitigation actions, contingency planning, and testing. Version 02C of this Security Directive issued in July 2022, marked a departure from a prescriptive approach, to a performance-based approach focused on the following outcomes:
    - Develop policies and controls for network segmentation to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised and vice-versa;
    - Create access control measures to secure and prevent unauthorized access to critical cyber systems.
    - Build continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect critical cyber system operations.
    - Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology.
  - IC Pipeline-2022-02,<sup>47</sup> Enhancing Pipeline Cybersecurity was issued to non-critical Pipeline owners and operators.
- TSA completed inspections to ensure compliance of all entities within the applicability of the Security Directive Pipeline-2021-01 series and Security Directive Pipeline-2021-02B.
- TSA conducted CSRs with 22 critical pipeline companies and CFSRs at 53 facilities to assess whether physical security measures adhered to guidance in the TSA Pipeline Security Guidelines. Since TSA issued the Security Directives, all the cybersecurity measures have been removed from the CSR process.

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

Objective 2.1: Intelligence and Information Sharing: Maintain and enhance mechanisms for information and intelligence sharing between the pipeline industry and government

Activity 2.1.1: Provide timely and relevant information and intelligence to enhance industry's domain awareness

### Key Accomplishments:

- TSA provided 58 intelligence and information sharing products to mass transit and passenger rail, freight rail, and pipeline stakeholders. The agency shared each product within 24 hours of release to keep industry informed about potential threats to transportation systems. TSA, CISA, FBI, and other sources produced intelligence

<sup>47</sup> Issued February 16, 2022.

products, such as advisories and information relating to potential vulnerabilities.

- TSA helped plan and execute a virtual International Pipeline Security Forum in October 2021. Forum included in TSA Administrator’s keynote address.
- TSA conducted 11 monthly calls with approximately 250 pipeline security personnel and provided updates on physical and cybersecurity threats and federal programs.
- TSA coordinated federal initiatives with federal partners and industry representatives at monthly meetings of the Energy GCC and Oil and Natural Gas SCC.
- TSA participated and provided a pipeline program update at quarterly meetings of the Joint Transportation GCC and SCC.
- TSA coordinated the Pipeline Cybersecurity Initiative (PCI) with the CISA National Risk Management Center (NRMC) including bi-weekly staff meetings and monthly briefings.
- TSA participated and provided an update on U.S. pipeline threats and initiatives at quarterly meetings of the Canadian Energy Utilities Sector Network (EUSN).

Objective 2.2: Community Outreach: Encourage industry engagement with first responders and the public to enhance understanding of community risks associated with pipeline systems

Activity 2.2.1: Promote pipeline security awareness in communities surrounding critical pipeline assets and systems

Key Accomplishments:

- TSA conducted on-site reviews of community outreach at 22 critical pipeline companies to assess their adherence to the community outreach guidance in the TSA Pipeline Security Guidelines.
- Seventy-five percent of pipeline companies assessed through CSRs were identified as meeting the TSA Pipeline Security Guidelines for community outreach events. CSRs are conducted on a three to five year rolling basis. Each year, a new set of stakeholders are assessed, which can result in a fluctuation of the final result percentages. Operators that are determined not to have implemented this objective as outlined in the Pipeline Security Guidelines, are provided with recommendations for community outreach. Since this review is non-regulatory, there is no civil enforcement for non-implementation.
- TSA provided Pipeline Operators Good Neighbors brochures to be distributed to residences and industry for security awareness and provided DVDs on the role of law enforcement and pipeline operators.
- TSA held monthly pipeline conference calls with approximately 200-300 pipeline stakeholders.

## D. Intermodal

The Intermodal domain involves the protection of supply chains across multiple modes of transportation including, trucking, rail, aviation, and maritime systems. The global supply chain is complex and expansive, often operating to provide time-sensitive deliveries. Disruptions to



intermodal operations in major gateway cities could result in significant social and economic consequences. Federal partners collaborate to streamline security processes on traded goods, manage risks to vulnerable assets and systems, assess the effectiveness of anti-terrorism measures within the global supply chain, and build stronger security capacity where gaps are identified.

**Table 7** shows key accomplishments related to the specific goals, objectives, and activities in the 2020 NSTS Intermodal.

**Table 7: Intermodal Progress Assessment**

<b>Goal 1: Manage risks to transportation systems from terrorist attack and enhance system resilience</b>
Objective 1.1: Manage risks from transportation vulnerabilities in vital supply chains
Activity 1.1.1: Identify and assess key supply chain transportation assets and systems
<p>Key Accomplishment:</p> <ul style="list-style-type: none"> <li>As noted in the FY 2020/2021 Annual Report on Transportation Security, the associated measures for this activity are no longer applicable, and are revised in the most recent version of the NSTS.</li> </ul>
Activity 1.1.2: Support state and local government to remediate physical security vulnerabilities of transportation operations to protect critical infrastructure
<p>Key Accomplishment:</p> <p>As noted in the FY 2020/2021 Annual Report on Transportation Security, the associated measures for this activity are no longer applicable, and are revised in the most recent version of the NSTS.</p>
Objective 1.2: Encourage adoption of global supply chain transportation-related standards, regulations, guidelines, and best practices
Activity 1.2.1: Implement the ISPS to assess the effectiveness of anti-terrorism measures in foreign ports, build security capacity where gaps exist, and impose conditions of entry on vessels arriving in the United States from ports with substandard security
<p>Key Accomplishment:</p> <ul style="list-style-type: none"> <li>Centers of Excellence and Expertise: These centers work with the international trade community to transform CBP’s approach to trade operations. These centers increase the use of uniform practices across ports of entry, help to resolve trade compliance issues nationwide in a timely manner, and further strengthen critical agency knowledge of key industry practices.</li> </ul>
<b>Goal 2: Enhance effective domain awareness of transportation systems and threats</b>
Objective 2.1: Enhance federal analysis and sharing of transportation security supply chain

information to improve situational awareness of terrorist threats
Activity 2.1.1: Implement advance notice of arrival protocols including CBP’s 24-Hour Advance Manifest Rule <sup>48</sup> and the USCG’s 96-Hour Advance Notice of Arrival to identify higher-risk cargo movements for enhanced security review
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• CBP worked to identify potential high-risk cargo prior to departure or upon arrival at a U.S. port of entry.</li> <li>• USCG used pre-loading advance cargo information to examine the application of advance cargo information and as a platform for dialogue among program participants and between regulators and industry.</li> </ul>
Activity 2.1.2: Develop cybersecurity-related incident and vulnerability reporting guidance for transportation systems sector stakeholders in alignment with the NIST Cybersecurity Framework, the National Cyber Incident Response Plan, and applicable law.
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• TSA developed a series of Security Directives (SD 1580-21-01, SD 1582-21-01, SD Pipeline-2021-01) and Emergency Security Program Amendments (EA) for regulated transportation systems sector owner/operators about criteria and processes for reporting cybersecurity incidents. TSA also issued ICs (Surface Transportation IC-2021-01, IC Pipeline-2022-02) that provided recommended guidance to non-regulated transportation stakeholders.</li> <li>• TSA’s incident reporting guidance in the SD/EAs and ICs aligned with the NIST Cybersecurity Framework v1.1 Respond Communication function (RS.CO) and CISA’s Cross-Sector Cybersecurity Performance Goal 4.A- Incident Reporting.</li> </ul>
Objective 2.2: Strengthen and grow stakeholder partnerships and collaboration on supply chain resilience
Activity 2.2.1: Streamlining security processes in collaboration with public and private sector partners to enhance U.S. economic competitiveness by enabling lawful trade
<p>Key Accomplishments:</p> <ul style="list-style-type: none"> <li>• CBP continues to operate several international trusted traveler programs that offer expedited processing for pre-identified, lower risk populations including, Secure Electronic Network for Travelers Rapid Inspection (SENTRI), NEXUS, Free and Secure Trade (FAST), and Global Entry. These programs provide modified screening for pre-approved members, improve security by increasing efficiencies in allocating screening resources, and facilitate legitimate trade and travel.</li> <li>• As of September 30, 2022:</li> </ul>

<sup>48</sup> CBP must receive, by way of a CBP-approved electronic data interchange system, information pertaining to cargo before the cargo is either brought in to or sent from the United States by any mode of commercial transportation (sea, air, rail, or truck). The cargo information required is that which is reasonably necessary to enable high-risk shipments to be identified for purposes of ensuring cargo safety and security and preventing smuggling pursuant to the laws enforced and administered by CBP.

- Over 619,000 SENTRI members accounted for 28 percent of cross-border traffic along the Southwest border;
- Over 1.6 million members are enrolled in the NEXUS program;
- Global Entry has reduced wait times more than 75 percent;
- Over 8.2 million participants are enrolled directly in Global Entry;
- Over 1.9 million members of NEXUS and SENTRI also receive Global Entry benefit. In addition, all Global Entry members are eligible for the TSA PreCheck<sup>®</sup> program. TSA PreCheck<sup>®</sup> provides expedited screening through U.S. airport security checkpoints via designated screening lanes.

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

Objective 3.1: Manage transportation risks in the global supply chain networks to promote the efficient flow of commerce

Activity 3.1.1: Expand risk segmentation through advanced technology to enable low-risk trade and travel (Automated Targeting System, Automated Manifest System, Air Cargo Advance Screening, and Customs Trade Partnership Against Terrorism (CTPAT)).<sup>49</sup>

#### **Key Accomplishments:**

- More than 75,000 commercial drivers are enrolled in the CBP FAST program nationwide. FAST enrollment is open to truck drivers from the U.S., Canada, and Mexico and provides benefits including, access to dedicated lanes for greater speed and efficiency in processing trans-border shipments; reduced number of inspections, resulting in reduced delays at the border; Priority, front-of-the-line processing for CBP inspections; and, Enhanced supply chain security while promoting the economic prosperity of the U.S., Canada, and Mexico. Participation in FAST requires that every link in the supply chain, from manufacturer to carrier to driver to importer, is validated under CTPAT.
- CBP routinely conducts on site visits to domestic and foreign CTPAT member facilities to evaluate and validate their supply chain security measures. More than 11,000 companies are certified CTPAT partners, all of whom, accounted for 51 percent (by value) of cargo imported into the United States in FY 2022. During that same period, 1,467 validations were completed to certify that the highest level of supply chain security measures were being followed as required. While over 98 percent of CTPAT members remained in good standing with the program, enforcement actions led to 101 suspensions and 127 removals.
- NEXUS, an expedited travel program for air, land, and sea border crossings along the northern border, is a partnership between the Canadian and U.S. governments, through

<sup>49</sup> CTPAT is a voluntary government-private sector partnership that establishes clear supply chain security criteria for members. Membership provides incentives and benefits like expedited processing. CTPAT is conducted in close cooperation with principal stakeholders of the international supply chain, and partners include U.S. importers, exporters, U.S./Canada highway carriers, U.S./Mexico highway carriers, rail, air and sea carriers, licensed U.S. Customs brokers, U.S. marine port authority/terminal operators, U.S. freight consolidators, third-party logistics providers (3PL), ocean transportation intermediaries and non-operating common carriers, Mexican and Canadian manufacturers, and Mexican long-haul carriers.

the Canada Border Services Agency, and CBP. As of July 2022, there are over 1.6 million members enrolled in the NEXUS program. NEXUS participants are vetted on an ongoing basis by both the Canada Border Services Agency (CBSA) and CBP.

Activity 3.1.2: Streamlining security processes in collaboration with public and private sector partners to enhance U.S. economic competitiveness by enabling lawful trade

Key Accomplishments:

- CBP consistently applied risk-based methodologies to protect U.S. revenue and identify those who try to evade U.S. trade laws. All 10 Centers of Excellence and Expertise (Centers), processed post-release trade activities on an account and industry-wide basis and targeted evasive and unfair trade practices. The Centers are the operational entity responsible for identifying, assessing and prioritizing risks within their respective industries with a focus on CBP’s priority trade issues. The Centers also administer the collection of trade remedies as well as lead and carry out operations to detect and deter unlawful trade activities.
- CBP builds and maintains partnerships with the trade community, using every opportunity to obtain industry knowledge and expertise to ensure facilitation of legitimate international trade. CBP conducted approximately 600 outreach engagements with U.S. manufacturers, importers and other members of the trade community to increase awareness of critical trade-related issues. Engagements included a combination of trainings, webinars, and industry-led conferences.

### III. Looking Forward

For over two decades, since the first report published in 2002,<sup>50</sup> TSA’s “Annual Report on Transportation Security” has documented the activities and accomplishments of the transportation sector. Many original reporting requirements have been completed, closed-out, or are managed and reported on by other federal agencies, as programs and processes have changed over the years.

The NSTS continues to evolve to address the dynamic changes in the TSS environment. Cybersecurity remains a top priority and is incorporated into the first overarching goal of the 2023 Biennial NSTS.<sup>51</sup> In an effort to streamline reporting, the National Strategy for Public Transportation Security (NSPTS) and the National Strategy for Railroad Transportation Security (NSRTS)<sup>52</sup> were incorporated into the surface modal plans. Specifically, the NSPTS was merged into the mass transit and passenger rail modal plans, and the NSRTS was merged into the freight rail security modal plans.

<sup>50</sup> The Aviation and Transportation Security Act contained the first annual reporting requirements.

<sup>51</sup> Goal 1 of the Biennial NSTS issued in April 2023 is: Manage Risks to Transportation Systems from Terrorist and Cyber-Attacks, and Enhance System Resilience.

<sup>52</sup> Required by sections 1404 and 1511 of the Implementing Recommendations of the 9/11 Commission Act of 2007 (9/11 Act), Pub. L. 110-53 (August 3, 2007) and incorporated into the modal security plans for Mass Transit and Passenger Rail, and Freight Rail in the NSTS. Requirements for reporting on the NSPTS and NSRTS per 6 U.S.C. § 1141, and 6 U.S.C. § 1161, are consolidated into the Annual Report on Transportation Security.

TSA will continue to seek ways to enhance performance metrics and reporting, such as bridging the activities of the TSA Modernization Act Section 1986(a)<sup>53</sup> with the NSTS modal objectives and continuing collaborative efforts with the TSS Co-SRMAs. By embracing innovation, expanding and enriching partnerships, and advancing deterrence and detection capabilities, we will maintain the freedom of movement that the traveling public and the Nation's commerce depend upon each day.

---

<sup>53</sup> Section 1986(a), Division K, TSA Modernization Act, of the FAA Reauthorization Act of 2018 (Pub. L. 115–254; 132 Stat. 3186; Oct. 5, 2018).

## Appendix A: Acronyms

AAR	American Association of Railroads
ACAS	Air Cargo Advance Screening
ADIAC	Aviation Domain Intelligence Integration and Analysis Cell
APTA	American Public Transportation Association
AMSP	Area Maritime Security Plan
AMSTEP	Area Maritime Security Training and Exercise Program
BASE	Baseline Assessment for Security Enhancement
CBP	United States Customs and Border Protection
CBSA	Canada Border Services Agency
CISA	Cybersecurity and Infrastructure Security Agency
Co-SRMA	Co-Sector Risk Management Agency
CFSR	Critical Facility Security Reviews
CSR	Corporate Security Reviews
CTPAT	Customs Trade Partnership Against Terrorism
CWMD	Countering Weapons of Mass Destruction Office
DOT	Department of Transportation
EUSN	Energy Utilities Sector Network
EXIS	Exercise Information System
FBI	Federal Bureau of Investigation
FAST	Free and Secure Trade
FE	Functional Exercise
FSE	Full Scale Exercise
FY	Fiscal Year
GCC	Government Coordinating Council
HD-AIT	High-Definition Advanced Imaging Technology
HMC	Highway and Motor Carrier
HME	Hazardous Material Endorsement
HSIN	Homeland Security Information Sharing Network
HTUA	High Threat Urban Area
IIR	International Industry Representative
I&A	Intelligence and Analysis
IC	Information Circular
ICAO	International Civil Aviation Organization
ICPS	Intelligence Community Production System
ICS	Industrial Control Systems
I-STEP	Intermodal Security Training and Exercise
KTN	Known Traveler Number
LPD	Last Point of Departure
MTPR	Mass Transit and Passenger Rail
NIST	National Institute of Standards and Technology
NRMC	National Risk Management Center
NSPTS	National Strategy for Public Transportation Security
NSTS	National Strategy for Transportation Security
NSRTS	National Strategy for Railroad Transportation Security

OSS	One Stop Security
OTRB	Over-the-Road-Bus
OTRB-ISAC	Over-the-Road-Bus-Information Sharing and Analysis Center
PCI	Pipeline Cybersecurity Initiative
PT-ISAC	Public Transportation - Information Sharing and Analysis Center
WMD	Weapons of Mass Destruction
RAMST	Risk Mitigation Activities for Surface Transportation
RD	Regional Directors
R&D	Research and Development
RSS	Regional Security Strategy
RSSM	Rail Security Sensitive Materials
SAIs	Security Action Items
SCC	Sector Coordinating Council
SD	Security Directive
SENTRI	Secure Electronic Network for Travelers Rapid Inspection
SETA	Security Enhancement Through Assessment
SISC	Surface Information Sharing Cell
SRMA	Sector Risk Management Agency
SSI	Sensitive Security Information
STSAC	Surface Transportation Security Advisory Committee
TIP	Threat Image Projection
TSA	Transportation Security Administration
TSAR	TSA Representatives
TSDS	Terrorist Screening Dataset
TSISE	Transportation Security Information Sharing Environment
TSS	Transportation Systems Sector
TSSRA	Transportation Sector Security Risk Assessment
TWIC	Transportation Worker Identification Credential
UAS	Unmanned Aircraft Systems
UK	United Kingdom
USCG	United States Coast Guard