United States Government Accountability Office

Report to Congressional Addressees

April 2020

PASSENGER RAIL SECURITY

TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices

GAO-20-404

GAO Highlights

Highlights of GAO-20-404, a report to congressional addressees

April 2020

PASSENGER RAIL SECURITY

TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices

Why GAO Did This Study

Recent physical and cyberattacks on rail systems in U.S. and foreign cities highlight the importance of strengthening and securing passenger rail systems around the world. TSA is the primary federal agency responsible for securing transportation in the United States.

GAO was asked to review TSA's efforts to assess passenger rail risk, as well as its role in identifying and sharing security standards and key practices. This report addresses (1) TSA's efforts to assess risk; (2) the extent to which TSA works with U.S. and foreign passenger rail stakeholders to identify security standards and key practices; and (3) the extent to which TSA shares passenger rail security standards and key practices with stakeholders.

GAO analyzed TSA risk assessments from fiscal years 2015 through 2019 and reviewed TSA program documents and guidance. GAO interviewed officials from TSA, and from seven domestic rail agencies, three foreign rail agencies, and two foreign government agencies. The results from these interviews are not generalizable but provide perspectives on topics in this review.

What GAO Recommends

GAO is making two recommendations: (1) that TSA update TSAR guidance to include engaging with foreign passenger rail stakeholders; and (2) that TSA update the BASE cybersecurity questions to ensure they reflect key practices. DHS concurred with both recommendations.

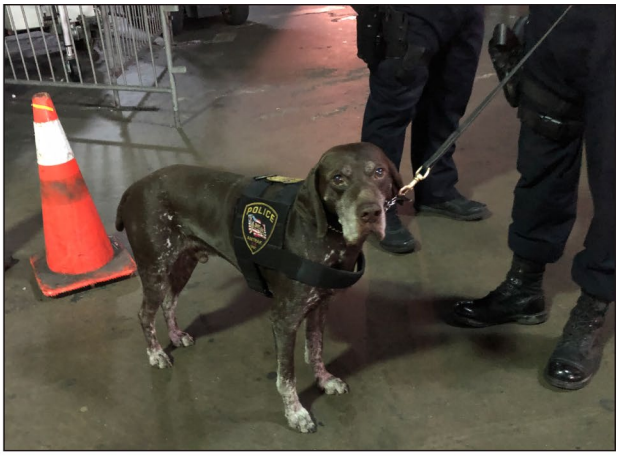
View GAO-20-404. For more information, contact Triana McNeil at (202) 512-8777 or mcneilt@gao.gov.

What GAO Found

The Transportation Security Administration (TSA) assesses passenger rail risks through the Transportation Sector Security Risk Assessment, the Baseline Assessment for Security Enhancement (BASE), and threat assessments. TSA uses the risk assessment to evaluate threat, vulnerability, and consequence for attack scenarios across various transportation modes. TSA surface inspectors use the baseline assessment, a voluntary security review for mass transit, passenger rail, and highway systems, to address potential vulnerabilities and share best practices, among other things.

TSA works with U.S. stakeholders to identify security standards and key practices and identifies foreign standards and practices through multilateral and bilateral exchanges. However, TSA Representatives (TSARs), the primary overseas point of contact for transportation security matters, lack specific guidance on foreign rail stakeholder engagement. As a result, TSA is less likely to be fully aware of key practices in other countries, such as station security guidance. Specific guidance would provide TSARs with clear expectations and encourage more consistent engagement with foreign rail stakeholders.

Examples of Security Key Practices Cited by Passenger Rail Stakeholders



Source: GAO. | GAO-20-404

Public Awareness Campaign
Emphasize security awareness

Canine Units
Detection of vapor from explosives

TSA shares standards and key practices with stakeholders, including those related to cybersecurity, through various mechanisms including BASE reviews; however, this assessment does not fully reflect current industry cybersecurity standards and key practices. For example, it does not include any questions related to two of the five functions outlined in the National Institute of Standards and Technology's Cybersecurity Framework—specifically the Detect and Recover functions. Updating the BASE questions to align more closely with this framework would better assist passenger rail operators in identifying current key practices for detecting intrusion and recovering from incidents.

Contents

Figures

Abbreviations

APTA	American Public Transportation Association
BASE	Baseline Assessment for Security Enhancement
CISA	Cybersecurity and Infrastructure Security Agency
DHS	Department of Homeland Security
NIPP	National Infrastructure Protection Plan
NIST	National Institute of Standards and Technology
RAILPOL	European Association of Railway Police Forces
TSA	Transportation Security Administration
TSAR	Transportation Security Administration Representative
TSSRA	Transportation System Sector Specific Risk Assessment

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

April 3, 2020

Congressional Addressees

Passenger rail systems are inherently difficult to secure and vulnerable to attack due to factors such as their open infrastructure, multiple access points, and high ridership.[1] Recent attacks in London, Brussels, and New York City, as well as planned attacks in New York and other U.S. cities, highlight the importance of strengthening and securing passenger rail systems around the world.[2] In addition, cyberattacks, such as those that affected San Francisco's mass transit system in 2016 and Deutsche Bahn in Germany in 2017, as well as derailment attempts in Germany in 2018, demonstrate the evolving nature of the threat to passenger rail.[3] In 2017, there were more than 4.8 billion passenger trips on rail systems in the United States. Rail operators and federal agencies are faced daily with the challenge of protecting passengers without compromising the accessibility and efficiency of rail travel. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) is the

[1]Passenger rail systems include heavy rail, light rail, commuter rail, and intercity rail. In 2017, there were 88 rail systems operated by public transit agencies in the United States. Most subway systems are considered heavy rail, which is an electric railway that carries a heavy volume of traffic, among other characteristics. Light rail systems typically operate passenger rail cars singly (or in short, usually two-car trains) and are driven electrically with power being drawn from an overhead electric line. Commuter rail is characterized by passenger trains operating on railroad tracks and providing regional service, such as between a central city and its adjacent suburbs. Intercity rail is primarily provided by the National Railroad Passenger Corporation (commonly known as Amtrak). For purposes of this review, we are using the term "passenger rail" to include all of these different types of passenger rail transit systems.

[2]A suicide bomber detonated a bomb on subway train in Brussels on March 22, 2016. On September 15, 2017, a bomb detonated on a London Underground train. On December 11, 2017, a pipe bomb detonated in a subway station adjoining the Port Authority Bus Terminal in New York. In addition, there have been multiple thwarted attacks against New York mass transit, including undetonated explosives that were found in a trash receptacle near a mass transit station in Elizabeth, New Jersey on September 18, 2016. Other foiled attacks occurred in Washington, D.C., and other U.S. cities.

[3]In 2016, a cyberattack affected transit ticketing and rail agency internal computer systems in San Francisco. In 2017, a global cyberattack (WannaCry) affected train scheduling information for the German rail operator Deutsche Bahn. In 2018, there were several unsuccessful attempts to derail trains in Germany, including by placing cement blocks on the tracks in one incident, and by stringing a steel rope across tracks in another incident.

primary federal agency responsible for securing all modes of transportation in the United States, including passenger rail.[4]

We previously reported on domestic and foreign passenger rail security practices and lessons learned in 2005 and 2012.[5] In 2005, we reported on, among other things, security practices that federal agencies and domestic and foreign rail operators had implemented, including foreign rail security practices that were not in use domestically at the time.[6] In 2012, we reported on the influence of foreign attacks on domestic rail security procedures, among other things. Further, though not specific to passenger rail cybersecurity, federal cyber asset security has been on our High Risk list since 1997. In 2003, we expanded this area to include protecting systems supporting our nation's critical infrastructure, such as passenger rail systems.[7] We issued an update to the information security

[4]Coast Guard is the lead federal agency responsible for maritime transportation security, though TSA plays a role in managing some security aspects.

[5]See GAO, *Passenger Rail Security: Enhanced Federal Leadership Needed to Prioritize and Guide Security Effort,* GAO-05-851 (Washington, D.C. Sept. 9, 2005) and GAO, *Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives*, GAO-13-20 (Washington, D.C.: Dec. 19, 2012).

[6]We reported on three practices observed in other countries that were not in use among domestic passenger rail operators at the time. These practices included (1) the use of covert testing to keep employees alert about their security responsibilities; (2) random screening of passengers and their baggage; and (3) central clearinghouses on rail security technologies and best practices. We recommended, among other things, that DHS and the Department of Transportation collaborate with the passenger rail industry to evaluate the potential benefits and applicability of implementing practices used by foreign rail operators. In response, TSA reported that it took actions to expand options for covert testing into the Intermodal Security Training Exercise Program and into Visible Intermodal Prevention and Response team activities and spearheaded an effort to compile effective security practices internationally. We determined that these actions addressed the intent of our recommendation. See GAO-05-851.

[7]Our biennial High Risk List identifies government programs that have greater vulnerability to fraud, waste, abuse, and mismanagement or need to address challenges to economy, efficiency, or effectiveness. We have designated federal information security as a High Risk area since 1997; in 2003, we expanded this high risk area to include critical cyber infrastructure protection; and, in 2015, we further expanded this area to include protecting the privacy of personally identifiable information that is collected, maintained, and shared by both federal and nonfederal entities. See GAO, *High Risk Series: Progress on Many High Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317 (Washington, D.C.: Feb. 15, 2017).

high-risk area in September 2018 that identified actions needed to address cybersecurity challenges facing the nation.[8]

The FAA Reauthorization Act of 2018 includes a provision for us to review TSA's efforts to identify and share domestic and foreign passenger transportation security standards and key practices, particularly as they relate to shared terminal facilities, which we refer to as intermodal stations throughout this report, and cybersecurity.[9] In addition, we were asked to review how TSA assesses passenger rail security risks. This report addresses the following objectives:

1. How does TSA assess risks to the U.S. passenger rail system?
2. To what extent does TSA work with U.S. and foreign passenger rail stakeholders to identify security standards and key practices, including intermodal station and cybersecurity practices?
3. To what extent does TSA share passenger rail security standards and key practices with stakeholders?

To address the first objective, we reviewed agency assessments and documentation pertaining to the elements of risk (threat, vulnerability, and consequence), as defined in the National Infrastructure Protection Plan (NIPP).[10] Specifically, we reviewed TSA's Transportation Sector Security Risk Assessment (TSSRA) from fiscal years 2015 through 2017,[11] documents related to TSA's Baseline Assessment for Security Enhancement (BASE), and TSA's annual and semiannual threat

[8]GAO, *High Risk Series: Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation*, GAO-18-622 (Washington, D.C.: Sept. 6, 2018).

[9]Pub. L. No. 115-254, § 1972, 132 Stat. 3186, 3614. The TSA Modernization Act is Division K, title I of the FAA Reauthorization Act of 2018. Intermodal stations are facilities or hubs where multiple modes of transportation intersect. For example, Washington D.C.'s Union Station, where Amtrak, subway, commuter rail, and buses converge, is an intermodal station. Intermodal hubs may be particularly vulnerable to attack due to factors such as open public areas, multiple vendors, large volumes of passengers, and limited escape routes.

[10]Department of Homeland Security, *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: December 2013).

[11]According to TSA officials, the 2017 TSSRA was the most recent available at the time we conducted our audit work.

assessments from calendar years 2015 through 2019.[12] In addition to reviewing general risks to the passenger rail system identified in these documents, we analyzed the extent to which they address intermodal station and cybersecurity risk. We conducted interviews with TSA officials responsible for TSA's passenger rail risk assessment efforts. We also conducted interviews with officials from DHS's Cybersecurity and Infrastructure Security Agency (CISA) to understand additional efforts to assess the cybersecurity risk in passenger rail, and how the agency coordinates with TSA.

To address objectives two and three, we obtained information in person or via telephone from officials at seven domestic rail agencies, including Amtrak.[13] We also conducted site visits to two foreign countries and interviewed government officials and officials from three passenger rail agencies in these countries.[14] We conducted these interviews and visits to obtain perspectives on both domestic and foreign passenger rail security standards and key practices, as well as TSA engagement in this area. To select domestic rail agencies, we first identified agencies with the largest passenger volume by type of agency (heavy, light, or commuter rail). We then selected specific agencies to interview based on the following factors: type of system, geographic diversity, the presence of a large intermodal station, expert referral, and experience with security threats or incidents. We selected the foreign countries we visited based on the size of passenger rail operations, presence of a large intermodal station, expert referral, and experience with security threats or incidents.[15] While the perspectives of rail agencies and officials we interviewed are

[12]The BASE is a voluntary security assessment of mass transit, passenger rail, and highway systems. We reviewed documents dating back to 2015 to understand how, if at all, passenger rail risk and TSA assessment efforts changed over time.

[13]The officials we interviewed represented the following agencies: Amtrak; Chicago Transit Authority; Los Angeles County Metropolitan Transportation Authority; Massachusetts Bay Transportation Authority; New York City Metropolitan Transit Authority; San Francisco Bay Area Rapid Transit; and Washington Metropolitan Area Transit Authority. One rail agency—the New York City Metropolitan Transit Authority—provided written responses to our questions.

[14]We visited the United Kingdom and Germany and conducted interviews with officials from the United Kingdom's Department for Transport, Network Rail, the British Transport Police, London Underground, and from Germany's Deutsche Bahn and Berliner Verkehrsbetriebe (which operates Berlin's U-Bahn subway system).

[15]We also considered logistical factors such as visa and translator requirements.

not generalizable to all rail agencies and countries, they provided a range of perspectives on the topics within the scope of our review.

To further address our second objective, we reviewed documentation from domestic and international rail security working groups and meetings, such as those hosted by the American Public Transportation Association (APTA), and the International Working Group on Land Transport Security, among others. We further reviewed all available security-related standards and recommended practice documents APTA produced from calendar years 2009 through 2019 to determine whether TSA participated in developing or reviewing the documents. In addition, we interviewed TSA officials as well as representatives from APTA, the Association of American Railroads, and the Mineta Transportation Institute to identify current threats, existing key practices in passenger rail security, and TSA's role in identifying these practices. To further understand TSA's efforts to engage with foreign passenger rail stakeholders, we interviewed TSA Representatives (TSARs) located in two countries we visited. We evaluated TSA's efforts against the NIPP, which outlines government and private sector partnerships needed to achieve security goals, TSA's *2018 Administrator's Intent*, and TSA program documentation.

To further address our third objective, we reviewed documentation from rail security working groups and meetings, such as those identified above. We also reviewed relevant documentation related to TSA programs such as the BASE, the Intermodal Security Training and Exercise Program, and the Visible Intermodal Prevention and Response program, to identify whether TSA shares key practices, including those learned from foreign stakeholders, through these programs. We interviewed TSA officials to discuss their efforts to share key practices with stakeholders. We also analyzed questions in the BASE assessment to identify the extent to which they incorporate cybersecurity key practices as identified in the National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity*.[16] We further assessed these efforts against TSA's *Transportation Systems Sector-Specific Plan*,

[16]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1 (Apr. 16, 2018).

which calls for the adoption of the NIST Framework across all transportation modes.[17]

We conducted this performance audit from July 2019 to April 2020 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

TSA and Industry Roles in Securing Passenger Rail

The Aviation and Transportation Security Act designated TSA as the primary federal agency responsible for security in all modes of transportation, which includes physical security and cybersecurity.[18] Passenger rail operators, however, have the day to day responsibility for carrying out safety and security measures for their systems. Unlike the aviation environment, where TSA has operational responsibility for screening passengers and baggage for prohibited items prior to boarding a commercial aircraft, the agency has a limited operational role for securing mass transit (including rail).[19] To secure passenger rail, TSA primarily partners with public and private transportation operators to address their security needs by conducting vulnerability assessments and sharing intelligence information and key practices, among other

[17]Department of Homeland Security and Department of Transportation, *Transportation Systems Sector-Specific Plan* (Washington, D.C.: 2015).

[18]Pub. L. No. 107-71, § 101(a), 115 Stat. 597 (2001) (codified at 49 U.S.C. § 114(d)). Pursuant to the Aviation and Transportation Security Act, TSA has authority to assess threats to transportation, develop policies, strategies, and plans for dealing with such threats, and enforce compliance with regulations and requirements. TSA may also issue, rescind, and revise such regulations as are necessary to carry out its transportation security functions. 49 U.S.C. § 114(f), (*l*)(1). Coast Guard is the lead federal agency responsible for maritime transportation security, though TSA plays a role in managing some security aspects. TSA is responsible for the following five transportation modes: mass transit and passenger rail; freight rail; highway; pipeline; and aviation.

[19]TSA provides operational support in the form of providing trained explosives detection canines to operators, and random baggage screening support. TSA also partners with mass transit and passenger rail operators through the Visible Intermodal Prevention and Response program to augment high visibility patrols with operators as a force multiplier.

measures.[20] The agency also engages with the passenger rail industry through associations, such as APTA and Association of American Railroads.[21] Additionally, TSA is responsible for assessing the risk from terrorism and cyber threats to passenger rail, as well as other transportation modes.

In addition to engaging with domestic passenger rail stakeholders, TSA's Office of Policy, Plans, and Engagement is responsible for coordinating domestic and international multimodal transportation security polices, programs, directives, strategies, and initiatives, including conducting outreach to foreign stakeholders. TSA also engages with foreign stakeholders through TSARs. TSARs are primarily located in posts overseas and communicate with foreign government officials to address transportation security matters involving all modes of transportation, including aviation, rail, mass transit, highways, and pipelines.[22] The TSAR role was originally created in response to the 1988 bombing of Pan Am Flight 103 over Lockerbie, Scotland, when the Aviation Security Improvement Act of 1990 was enacted, which provided that foreign security liaison officers were to serve as liaisons to foreign governments in carrying out U.S. government security requirements at specific airports.[23] TSARs are responsible for ensuring the implementation of TSA's requirements primarily as they relate to passenger and cargo air transportation departing the specific country en route to the United States. The primary focus of the role remains on aviation; however it has evolved over time to include maritime and land transportation.

Physical and Cybersecurity Threats to Passenger Rail

According to TSA, recent attacks overseas and online terrorist messaging point to public transportation systems, which include passenger rail

[20]TSA has issued a limited number of requirements for mass transit and passenger rail operators, including that rail carriers designate a rail security coordinator and report significant security concerns. See 49 C.F.R. §§ 1580.201, .203. TSA surface inspectors are to enforce these regulations through regulatory inspections.

[21]APTA is a trade association that represents all modes of public transportation, including bus, light rail, commuter rail, subways, waterborne services (such as ferries), and inter-city passenger rail (including Amtrak). The Association of American Railroads is a trade association that represents the freight rail industry, as well as Amtrak.

[22]According to TSA officials, there are 27 TSARs in locations around the world, including three in Miami; one additional TSAR position was vacant as of January 2020.

[23]See 49 U.S.C. § 44934.

systems, as continued high-value targets for terrorists.[24] In general, passenger rail systems are open and designed to expedite the free flowing movement of large numbers of passengers through multiple stations. As such, these systems are inherently vulnerable to physical attacks (such as improvised explosive devices, active shooters, and chemical or biological attacks) due in part to factors such as high ridership, open access points, limited exit lanes, and fixed, publically available schedules. In addition, TSA has reported that risks increase in urban areas where multiple transportation systems and high volumes of travelers merge at intermodal stations.

Transportation systems, including passenger rail systems, rely on technology and internet-connected devices to manage and secure certain business/enterprise functions, such as the operation's website, communications, and reservations and ticketing mechanisms. They also increasingly rely on computer-networked systems for tracking, signals, and operational controls of transportation equipment and services. As dependence on these systems increases, so does risk to the system. Cyberattacks have the potential to significantly affect both business/enterprise systems and operational control systems.[25]

- **Business/Enterprise systems.** Cybersecurity threats include ransomware, malware, phishing, and website attacks that may compromise sensitive information and affect an operator's ability to communicate with passengers or engage in day-to-day business functions.[26]
- **Operational control systems.** Cybersecurity threats, which may include malware or physical manipulation of a system, such as jamming signals or damaging equipment, include threats to the

[24]Transportation Security Administration, *Biennial National Strategy for Transportation Security: Report to Congress* (Washington, D.C.: Apr. 4, 2018).

[25]American Public Transportation Association, *Cybersecurity Considerations for Public Transit* (Washington, D.C.: Oct. 17, 2014.

[26]Ransomware is malicious software used to deny access to IT systems or data until a ransom is paid. Phishing is a digital form of social engineering that uses authentic-looking, but fake, emails to request information from users or direct them to a fake website that requests information. Malware, also known as malicious code and malicious software, refers to a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or otherwise annoying or disrupting the victim. Examples include logic bombs, Trojan horses, viruses, and worms.

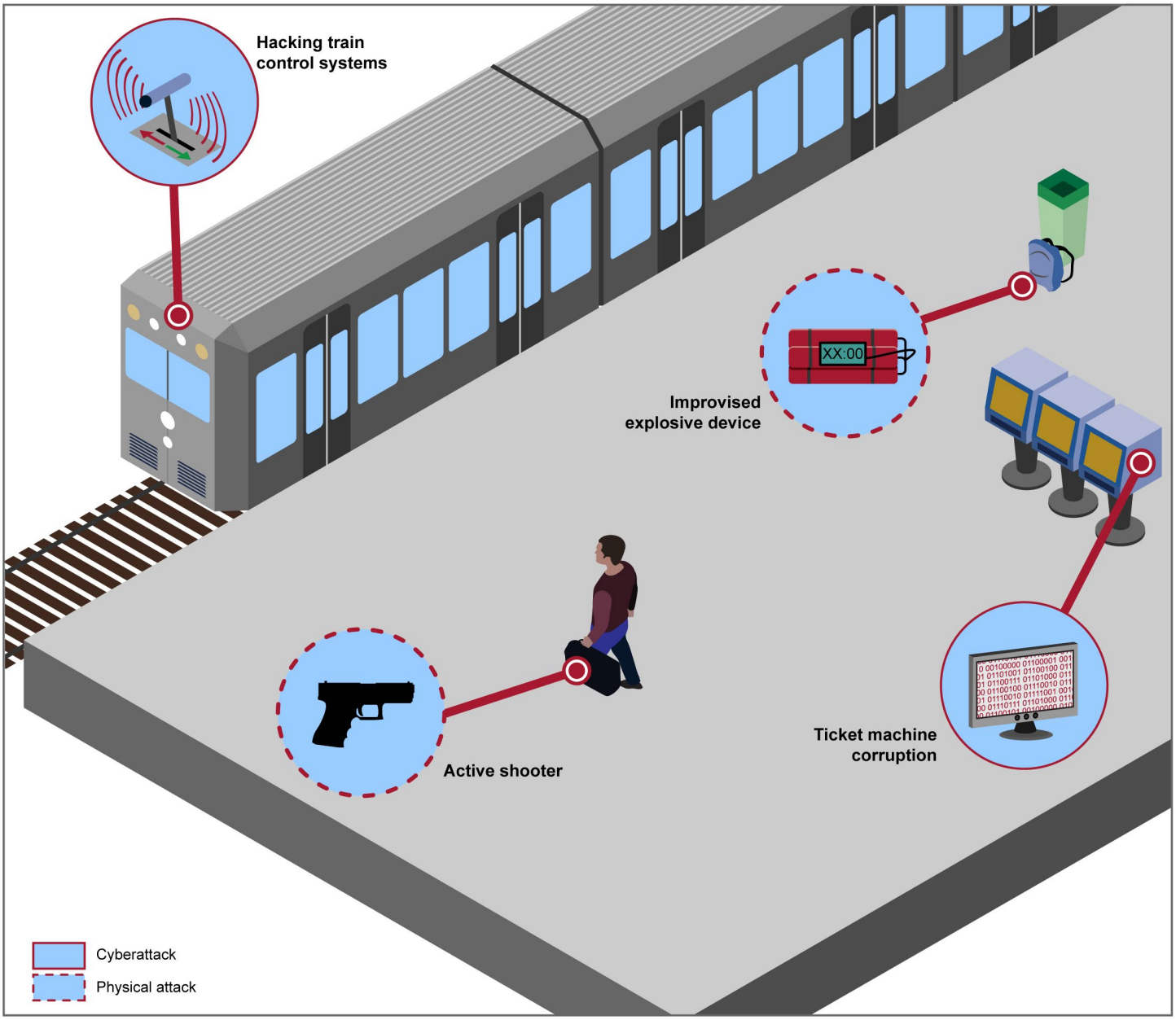
systems that control signaling and train speed.[27] For example, attackers could attempt to access positive train control systems, a computer-based system designed to automatically slow or stop a train that is not being operated safely, to disrupt services.[28]

Unintentional cybersecurity threat sources may include failures in equipment or software due to aging or user errors, such as unintentionally inserting a flash drive infected with malware or clicking on a phishing email. Intentional cybersecurity threats may include corrupt employees, criminal groups, terrorists, and nations and may be used, for example, to achieve monetary gain, or for political or military purposes. Figure 1 shows examples of the types of physical and cyber threats passenger rail systems face.

[27]Passenger rail systems may be monitored and operated through Supervisory Control and Data Acquisition systems, which is one type of computer-based control system that performs a range of simple to complex functions. Control systems such as these are vulnerable to cyberattacks from inside and outside the network. Once accessible to an attacker, such systems can be exploited in a number of ways to carry out a cyberattack, including issuing unauthorized commands to control equipment and delaying or blocking the flow of information through the network. Congressional Research Service, *Cybersecurity for Energy Delivery Systems,* R44939 (Washington, D.C.: Aug. 28, 2017).

[28]Forty-two railroads are required to implement positive train control by December 31, 2020, including 30 commuter railroads, Amtrak, and several freight railroads. We have previously reported on railroads' progress implementing positive train control, including challenges with interoperability and securing wireless communication. See, for example, GAO, *Positive Train Control: Most Railroads Expect to Request an Extension, and Substantial Work Remains Beyond 2018*, GAO-18-692T (Washington, D.C.: Sept. 13, 2018) and *Positive Train Control: As Implementation Progresses, Focus Turns to the Complexities of Achieving System Interoperability*, GAO-19-693T (Washington, D.C.: Jul. 31, 2019). The Federal Railroad Administration requires that positive train control wireless railroad communications be encrypted; however, in 2019 we reported that a solution to encrypt all wireless communications and data transmittal in the Northeast is currently in lab development. See 49 C.F.R § 236.1033 and GAO-19-693T.

Figure 1: Examples of Physical and Cybersecurity Threats to Passenger Rail

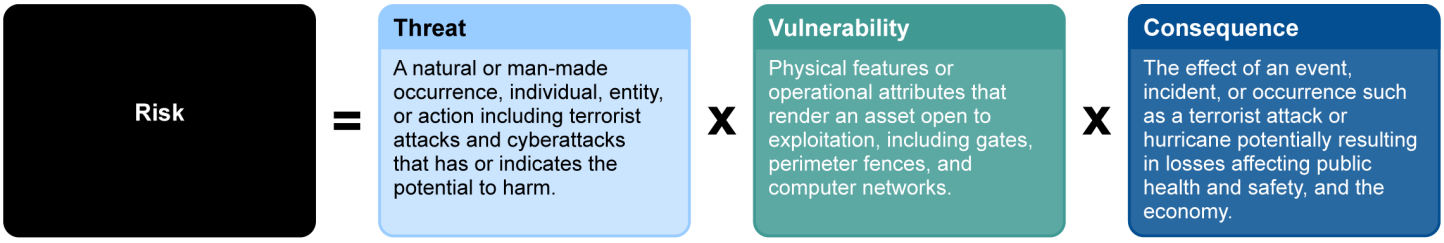


Source: GAO analysis of Transportation Security Administration information. | GAO-20-404

DHS Risk Management Framework

The NIPP outlines a risk management framework for critical infrastructure protection. In accordance with the Homeland Security Act of 2002, as amended, DHS created the NIPP in 2006 to guide the national effort to manage security risk to the nation's critical infrastructure, including through coordination of agencies and 16 various critical infrastructure sectors, including transportation systems.[29] Most recently updated in 2013, the NIPP uses a risk management framework as a planning methodology intended to inform how decision makers take actions to manage risk. The framework calls for public and private partners to conduct risk assessments. The NIPP defines risk as a function of three elements: threat, vulnerability, and consequence, as shown in Figure 2. Threat is an indication of the likelihood that a specific type of attack will be initiated against a specific target or class of targets. Vulnerability is the probability that a particular attempted attack will succeed against a particular target or class of targets. Consequence is the effect of a successful attack.

Figure 2: Elements of Risk Related to Infrastructure Protection



Source: GAO analysis of the Department of Homeland Security's National Infrastructure Protection Plans (2009 and 2013). | GAO-20-404

[29]See Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2135, 2146. Presidential Policy Directive 21, issued in February 2013, was developed to advance a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive identifies the 16 critical infrastructure sectors and assigns roles and responsibilities for each sector. The 16 critical infrastructure sectors include: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; healthcare and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems.

In 2010, DHS, through TSA and the U.S. Coast Guard, developed the *Transportation Systems Sector-Specific Plan* to conform to requirements in the NIPP.[30] Most recently updated in 2015, this plan describes shared goals, priorities, and activities to mitigate critical infrastructure risks, and acknowledges the increasing dependence of transportation companies on cyber systems for business, security, and operational functions.

Regarding cybersecurity risks, DHS produced the *Cybersecurity Strategy* in 2018 to help execute its cybersecurity responsibilities during the next 5 years.[31] In order to meet one of its objectives, DHS is to encourage the adoption of applicable cybersecurity best practices, including the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (referred to as the NIST Cybersecurity Framework). The framework is a set of voluntary industry standards and best practices to help organizations manage security risks specific to cybersecurity.[32] The framework consists of five functions: Identify, Protect, Detect, Respond, and Recover. When considered together, these functions provide a high-level view of an organization's management of cybersecurity risk. NIST issued the framework in 2014 and updated it in April 2018.[33]

CISA, formerly DHS's National Protection and Programs Directorate, manages the national effort to secure and protect against critical infrastructure risks, including cybersecurity risk, for all 16 critical

[30]The NIPP requires sector-specific agencies to develop strategic risk management frameworks for their sectors. TSA and the U.S. Coast Guard were the co-sector-specific agencies for the transportation systems sector in 2010. Presidential Policy Directive 21 added the Department of Transportation as a co-sector specific agency for the transportation systems sector in February 2013.

[31]Department of Homeland Security, *Cybersecurity Strategy* (Washington, D.C.: May 15, 2018).

[32]NIST issued the Cybersecurity Framework in response to Executive Order 13636, issued in 2013, which, among other things, called for NIST to lead the development of a framework to reduce cybersecurity risks to critical infrastructure. Exec. Order No. 13,636, 78 Fed. Reg. 11,737 (Feb. 19, 2013).

[33]National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014); *Framework for Improving Critical Infrastructure Cybersecurity* Version 1.1 (Apr. 16, 2018).

infrastructure sectors, including transportation.[34] CISA's responsibilities include coordinating with sector-specific agencies to carry out its cybersecurity and critical infrastructure activities.

TSA Conducts Passenger Rail Risk Assessments and Coordinates with CISA on Cybersecurity Risk

TSA Uses Three Mechanisms to Assess Passenger Rail Risk

According to TSA officials, TSA uses the TSSRA, the BASE, and threat assessments to assess risk elements for physical and cyber security in passenger rail. Such assessments may address different elements of risk—threat, vulnerability, or consequence—or the total risk for specific assets, such as airport perimeters and pipeline critical facilities. Table 1 below shows the type of risk element each assessment addresses, and whether the assessment addresses risks to intermodal stations or cybersecurity risk.

[34]The Cybersecurity and Infrastructure Security Agency Act of 2018, enacted November 16, 2018, amended the Homeland Security Act of 2002 by, among other things, re-designating the DHS National Protection and Programs Directorate as the Cybersecurity and Infrastructure Security Agency (CISA) with responsibility for, among other things, leading cybersecurity and critical infrastructure security programs, operations, and associated policy for CISA, including national cybersecurity asset response activities, and coordinating with federal entities, including sector-specific agencies and non-federal entities to carry out the cybersecurity and critical infrastructure activities of CISA. See Pub. L. No. 115-278, § 2(a), 132 Stat. 4168, 4169 (codified at 6 U.S.C. § 652).

Table 1: Mechanisms the Transportation Security Administration (TSA) Uses to Assess Risk Elements for Passenger Rail

Assessment	Risk element(s)	Addresses intermodal stations[a]	Addresses cybersecurity
Transportation Sector Security Risk Assessment (TSSRA) – a risk assessment for attack scenarios across the five transportation modes for which TSA is responsible.	Threat, vulnerability, and consequence	Yes	No[b]
Baseline Assessment for Security Enhancement (BASE) – a voluntary assessment of mass transit, passenger rail, and highway systems.	Vulnerability	Yes[c]	Yes
Threat Assessments – annual and semiannual assessments that identify security threats to mass transit and passenger rail systems.	Threat	Yes[d]	Yes

Source: GAO analysis of TSA documents. | GAO-20-404

[a]Intermodal stations are facilities or hubs where multiple modes of transportation intersect.

[b]According to TSA officials, TSA plans to add cybersecurity scenarios to the TSSRA in fiscal year 2020.

[c]The BASE does not contain questions that directly refer to intermodal stations, as, according to TSA officials, the BASE is intended to assess an operator's overall security posture, including vulnerability, as opposed to the security posture at specific stations or facilities. Questions in the BASE do, however, address topics that selected domestic rail agencies we interviewed identified as key to intermodal station security.

[d]TSA's threat assessments do not directly address intermodal stations, though stations in general, which can include intermodal stations, are mentioned when they are the subject of an attack.

TSSRA. TSA uses the TSSRA, a periodic risk assessment, to assess threat, vulnerability, and consequence for various attack scenarios across the five transportation modes for which TSA is responsible.[35] The scenarios define a type of threat actor—including homegrown violent extremists and transnational extremists, such as Al Qaeda and its affiliates—a target, and an attack mode. For example, a scenario might assess the risk of attacks using varying types of weapons on passenger rail system assets. As part of the assessment process, TSA engages with subject matter experts from TSA and industry stakeholder representatives to compile vulnerabilities for each mode, and TSA analyzes both direct and indirect consequences of the various attack scenarios.[36] According to TSA, the agency uses the TSSRA to provide strategic insights to inform the administration's risk mitigation strategies, policy considerations, security countermeasures and programs, and resource allocation decisions.[37]

[35]According to TSA officials, the TSSRA has been issued with various frequencies. For example, TSA issued the TSSRA annually from calendar years 2015 through 2017. TSA officials stated that after the 2020 TSSRA, TSA plans to issue the TSSRA biennially with limited threat update and special issues in the interim years. TSA developed the TSSRA in June 2010 in response to requirements to conduct risk assessments for the Transportation Systems sector, and to fulfill TSA's operational and strategic need for a comprehensive risk assessment to aid in planning, risk-based decision making, and resource allocation, as well as in response to our recommendation in a March 2009 report. See GAO, *Transportation Security: Comprehensive Risk Assessments and Stronger Internal Controls Needed to Help Inform TSA Resource Allocation*, GAO-09-492 (Washington, D.C.: Mar. 27, 2009); and Pub. L. No. 110-53, § 1511, 121 Stat. 266, 426-29 (2007) (codified at 6 U.S.C. § 1161) (requiring the submission of a nationwide risk assessment of a terrorist attack on railroad carriers).

[36]According to TSA, direct consequences include costs that are the immediate result of an event, with an immediate to one-year outlook focused on deaths and infrastructure damage; indirect consequences include secondary costs of an event, such as long-term effects on the industry and cascading effects on other industries, with a one to ten-year systemic outlook focusing on economic and policy implications.

[37]In 2017, we reported that TSA did not fully align surface transportation inspector activities with identified risks, and did not incorporate risk assessment results when planning and monitoring activities. We recommended that the TSA Administrator ensure that surface inspector activities align more closely with higher-risk modes by incorporating the results of surface transportation risk assessments, such as the TSSRA, when it plans and monitors surface inspector activities. TSA concurred with our recommendation and in March 2018 the Surface Compliance Branch updated the Compliance Program Manual to include language stating surface inspectors should consider risk as identified in the TSSRA and modal threat assessments when planning surface activities. See GAO, *Transportation Security Administration: Surface Transportation Inspector Activities Should Align More Closely With Identified Risks,* GAO-18-180 (Washington, D.C.: Dec. 14, 2017).

Our analysis of the TSSRAs issued during calendar years 2015 through 2017 indicates that TSA included intermodal station attack scenarios, but did not include cybersecurity scenarios. Specifically, the assessments featured various scenarios that targeted intermodal stations, which could include rail systems. For example, a scenario might describe attacks using various numbers of improvised explosive devices on an intermodal station. TSA did not include cybersecurity attack scenarios in the calendar year 2015, 2016, or 2017 assessments. According to the 2016 assessment and TSA officials we interviewed, threat experts have indicated that cyber threats, due to their unique nature and other factors, do not lend themselves to traditional TSSRA attack scenarios. However, as discussed below, the agency does conduct cyber threat assessments. Further, TSA's *Cybersecurity Roadmap 2018*, states that, as one objective, the agency will include cybersecurity in its risk assessments for all modes.[38] According to TSA officials, the implementation plan for the Roadmap, which was approved in September 2019, provides guidance and direction for meeting this objective. TSA officials confirmed that they plan to include basic cybersecurity scenarios for all modes in the 2020 TSSRA, and that they plan to engage with TSA mass transit experts and consult with industry experts as needed to inform future cyberattack scenarios.

BASE. The BASE is a voluntary security assessment of national mass transit, passenger rail, and highway systems conducted by TSA surface transportation inspectors that addresses potential vulnerabilities, among other things.[39] It consists of an assessment template with 17 security action items developed by TSA and the Federal Transit Administration that address, among other best practices, security training programs, risk information sharing, and cybersecurity. TSA developed this assessment in 2006 to increase domain awareness, enhance prevention and protection capabilities, and further response preparedness of passenger transit systems nationwide.[40] The agency uses the BASE assessments to

[38]The TSA Cybersecurity Roadmap identifies four cybersecurity priorities and six goals that will direct TSA's efforts to improve its protection of its internal information technology systems as well as the nation's transportation systems. See, Transportation Security Administration, *TSA Cybersecurity Roadmap 2018* (Washington, D.C.: 2018).

[39]The BASE is a non-regulatory security assessment, which requires surface transportation entities' voluntary participation.

[40]Initially, the BASE was designed to assess large mass transit entities in major metropolitan areas that transported 60,000 riders or more daily. In 2012, TSA expanded the BASE to the highway mode to include trucking, motor coach, and school bus operators.

track progress in implementing specific security measures over time, offer technical assistance and share best practices to help improve the overall security posture of agencies, and inform transportation security grant funding by, among other things, identifying actions agencies have taken to reduce vulnerability.

TSA officials stated that the most recent formal update to the assessment template began in 2014 and was fully implemented in 2015. The update included, among other changes, revised guidance for TSA surface inspectors and the addition of questions concerning active shooter events.[41] In fiscal year 2016, the agency also developed a more targeted BASE assessment that focuses the assessment on an entity's areas of concern as identified by surface inspectors in a previous BASE review of that operator. As of 2017, TSA had completed initial and follow-up assessments for the top 100 mass transit agencies in the country, which comprise approximately 80 percent of the ridership in the United States. TSA officials told us that their goal is to conduct follow-up assessments every one to three years.[42]

As previously shown in table 1, our analysis of the BASE template for mass transit and passenger rail indicates that it includes questions that address selected rail agency concerns about intermodal station security, and questions related to cybersecurity issues. Specifically, we found that

[41]In fiscal year 2014, TSA established a panel comprised of mass transit experts to adjust the BASE template by modifying topics and removing outdated questions in an effort to improve the quality and applicability of the assessments for industry stakeholders.

[42]TSA provides data from BASE assessments to the Federal Emergency Management Agency for use in its risk model that informs the Transit Security Grant Program. The program is a Department of Homeland Security grant program that provides funds to owners and operators of transit systems (which include intra-city bus, commuter bus, ferries, and all forms of passenger rail) to protect critical surface transportation infrastructure and the traveling public from acts of terrorism and to increase the resilience of transit infrastructure. In 2012, the Federal Emergency Management Agency updated the grant program's risk formula to include a distinct vulnerability component, developed in coordination with TSA, in response to our recommendation in a June 2009 report. The vulnerability component, which includes BASE assessment scores, was independently verified by GAO. The updated model provides a means for the Federal Emergency Management Agency to justify lower funding as a result of actions taken by agencies to reduce vulnerability. See GAO, *DHS Allocates Grants Based on Risk, but Its Risk Methodology, Management Controls, and Grant Oversight Can Be Strengthened*, GAO-09-491 (Washington, D.C.: June 8, 2009). In addition to providing BASE assessment scores, TSA also provides inputs, such as mass transit ridership numbers and track miles, to help calculate consequence. According to TSA officials, they also work with the Federal Emergency Management Agency to inform grant priorities.

while the template does not contain security action items or questions that directly refer to intermodal stations, questions in the template do correspond to topics that domestic rail agencies we interviewed identified as significant to intermodal station security, such as coordination among security forces, visible security measures, and establishing roles and responsibilities.[43] For example, one BASE question asks if the agency's system security plan has procedures or protocols for responding to security events with external agencies such as law enforcement or fire departments. This question corresponds to the challenge of coordination among security forces in intermodal stations identified by six of the seven agencies we interviewed.

Cybersecurity is the focus of one of the security action items, which includes a series of general questions related to whether the transit agency has developed a comprehensive cybersecurity strategy. According to TSA officials, the agency added cybersecurity questions to the BASE in 2013 and the questions are intended to be a high level review. For example, the BASE addresses whether the transit agency has conducted a cybersecurity risk assessment, ensured employee training covers cybersecurity roles and threats, and established a protocol for reporting cyber incidents. It also provides a list of available cybersecurity resources for agencies to consult.

Threat Assessments. TSA's Intelligence and Analysis Office identifies security threats to mass transit and passenger rail systems through various threat assessments, including annual and semiannual Mass Transit and Passenger Rail Terrorism Threat Assessments and annual Cyber Modal Threat Assessments.[44]

- TSA's Mass Transit and Passenger Rail Terrorism Threat Assessment is produced annually and establishes the current mass transit passenger rail threat level and reviews terrorist threats against mass transit passenger rail for the past year. Threat information includes terrorist attacks on passenger rail trains, train tracks, buses, bus stops, and various stations. Additionally, the threat assessment

[43]According to TSA officials, the BASE is intended to assess an operator's overall security posture, not the security posture at specific stations or facilities. Six of the seven domestic rail agencies we interviewed cited coordination among security forces as an issue for intermodal stations; three cited visible security measures; and four cited establishing roles and responsibilities.

[44]TSA Intelligence and Analysis provides threat estimates that inform threat elements in the TSSRA.

analyzes intelligence gaps for the mass transit mode. TSA supplements the annual assessment with a semiannual threat assessment that reviews terrorist threats against mass transit and passenger rail for a 6-month period. Our analysis of threat assessments TSA issued for calendar years 2015 through 2019 indicates that they addressed stations, in general, and intermodal stations specifically, when they are the subject of an attack. For example, an attack on Manchester, England's Victoria station, an intermodal station, was included in the 2018 Mass Transit and Passenger Rail Terrorism Threat Assessment.

- TSA's Cyber Modal Threat Assessment reviews cyber threats to transportation over the course of the previous year, establishes cyber threat levels for the transportation modes for which TSA is responsible, and evaluates the threat through the next year or two. This annual assessment examines cyber threats to business and industrial control systems from state and non-state actors, including terrorist groups, pro-terrorist hacker groups, and hacktivists.[45] Moreover, it analyzes incidents of cyberattacks and cyber espionage against U.S. and foreign transportation.

Both assessments analyze threat actors and their capabilities, intent, and activities—including attacks occurring internationally—as well as tactics, techniques, and procedures that could be employed in future attacks. TSA calculates threat levels for transportation and cyber modes based on assessments of threat actor intent and capability. It may also issue additional situation-based products on emerging threats. TSA routinely shares these threat assessments with rail agencies and other stakeholders, such as industry security professionals.

TSA Coordinates with CISA to Facilitate Voluntary Cybersecurity Assessments and Industry Outreach

In addition to TSA's risk assessment efforts, the agency coordinates with CISA, which conducts voluntary cybersecurity assessments as needed and requested by TSA and industry stakeholders.[46] Specifically, CISA offers eight different voluntary cyber assessment options for public and private sector stakeholders, including mass transit and passenger rail

[45]A hacktivist is an individual or group of individuals that commits a crime by illegally gaining access to or altering computer systems in order to further an ideological goal.

[46]CISA's cybersecurity assessment services are offered on a voluntary basis and are available upon request from industry stakeholders.

agencies.[47] Because CISA provides services to all 16 critical infrastructure sectors, including the transportation systems sector, officials noted that it must balance the resources it devotes to each sector. For example, CISA officials stated that they have conducted six Validated Architecture Design Review assessments on rail agencies since 2015, and currently have four pending requests from transportation agencies.[48] The Validated Architecture Design Review evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner.[49] CISA officials also stated that they have conducted weekly vulnerability scans for one rail agency since 2015.[50]

While CISA coordinates with federal and private sector stakeholders to identify and address significant risks to critical infrastructure through its assessments, agency officials stated that they defer to TSA (as the co-sector specific agency for transportation) to take the lead in broader cyber initiatives and outreach to the transportation sector. For example, TSA officials stated that the agency included CISA in planning its cybersecurity workshops, a series of half-day workshops for surface transportation agencies to learn about cybersecurity resources from DHS and discuss nontechnical cybersecurity actions to improve their cybersecurity posture. According to TSA's *Cybersecurity Roadmap 2018*, the agency plans to

[47]CISA offers the following cyber assessments: 1) Cyber Resilience Review; 2) External Dependencies Management Assessment; 3) Cyber Infrastructure Survey; 4) Phishing Campaign Assessment; 5) Risk and Vulnerability Assessment; 6) Remote Penetration Testing; 7) Vulnerability Scanning; 8) Validated Architecture Design Review.

[48]According to CISA officials, in fiscal year 2019, the agency staffed and budgeted 50 Validated Architecture Design Review assessments, 20 of which involved the transportation sector, specifically aviation and pipelines.

[49]The Validated Architecture Design Review encompasses architecture and design review, system configuration, log file review, and analysis of network traffic to develop a detailed representation of the communications, flows, and relationships between devices in order to identify anomalous communication flows. Reviews are based on standards, guidelines, and best practices and are designed for operational technology and information technology environments. After the review, the organization receives an in-depth report that includes findings and recommendations for improving operations and cybersecurity.

[50]Vulnerability Scanning (formerly known as Cyber Hygiene Scanning) is an external remote scanning of internet-accessible systems for known vulnerabilities on a continual basis. CISA performs regular network and vulnerability scans and delivers a weekly report to the requesting organization. The report details current and previously mitigated vulnerabilities and recommendations for migrating vulnerabilities uncovered during vulnerability scans.

assess the resilience of the transportation modes to malicious cyber activity in conjunction with CISA, among other things.

According to officials, TSA and CISA are collaborating or planning to collaborate on several cybersecurity assessments for passenger rail systems, including a cyber risk assessment for passenger rail cars and a cyber assessment of the mass transit and passenger rail mode. CISA officials told us that TSA, DHS's Science and Technology Directorate, and CISA's National Risk Management Center are in early phases of developing a cyber risk assessment for select passenger rail cars that they plan to produce in fiscal year 2020.[51] CISA officials stated that they intend to address cyber vulnerability in the rail car assessments and plan to reach out to operators to discuss results.

TSA officials told us that TSA and CISA also are considering a mass transit and passenger rail cyber assessment similar to one being developed for the pipeline mode. CISA officials stated that the planned pipeline assessment effort will include a total of 10 Validated Architecture Design Review assessments, in which TSA will help make arrangements with industry and will observe the process. TSA officials explained that expanding this effort to include passenger rail would depend on CISA's availability to conduct assessments and balance demands in other sectors. CISA officials noted that they currently do not have the resources to support a similar plan for rail.

[51]The National Risk Management Center is a planning, analysis, and collaboration center working to identify and address the most significant risks to critical infrastructure.

TSA Actively Works with Domestic Stakeholders to Identify Standards and Key Practices but Provides Limited Guidance on Foreign Stakeholder Engagement

TSA Works with Stakeholder Groups to Develop Domestic Standards and Recommended Practices

TSA participates in APTA working groups that review and develop standards and recommended practices for passenger rail security, including those that apply to intermodal station security and cybersecurity.[52] Specifically, from 2009 through 2019, APTA produced 45 documents related to security and emergency management standards and recommended practices, among other things. TSA is listed as a participant in 37 of the 45 documents.[53] TSA officials noted that APTA working groups regularly review documents and issues related to security topics, including through monthly phone calls in some cases, and update them as needed.[54] According to APTA's *Manual for the Standards Development Program*, standards address safety-critical subjects and establish requirements that must be met by industry;[55] recommended

[52]APTA produces documents that apply to all public transportation modes, including passenger rail. The APTA *Manual for the Standards Development Program* describes a standardized process for developing six types of documents, including: standards, recommended practices, guidelines, white papers, technical specifications, and training/educational materials. APTA produces general facility and station security standards and recommended practices that, according to APTA officials and our analysis, apply to intermodal stations, but are not specifically directed at that those facilities.

[53]According to a TSA official, TSA staff also participated in an additional six recommended practices where they were not listed as participants. The official further noted that because TSA primarily serves in a supporting role to ensure that standards and recommended practices do not conflict with any regulatory requirement, TSA staff names may not be listed in some cases.

[54]The ATPA manual states that documents are to be reviewed and updated as necessary every five years.

[55]Compliance with standards is voluntary. APTA does not enforce compliance – rather, standards enforcement is the responsibility of individual transit systems.

practices describe an established or generally recommended approach that does not rise to the level of a standard; and white papers are intended to provide information about complex issues that present the industry's prevailing philosophy on the subject matter.[56] For example:

- APTA offers a series of general standards, recommended practices, and white papers targeted at physical infrastructure protection at passenger facilities. These documents are not specifically directed at intermodal stations, but, according to our analysis and APTA officials, apply to such facilities as well as others. The documents address factors such as exterior door and window security, as well as securing mailrooms and utility openings, among other issues. Another APTA standard addresses security and emergency management considerations during planned special events, such as identifying transit hubs that are likely to be inundated with passengers going to and from the event.
- APTA offers cybersecurity recommended practices that are targeted at transit agencies in the early stages of starting a cybersecurity program, including how to obtain executive-level awareness and support and how to develop a cybersecurity awareness and training program. APTA also offers recommended practices for securing control and communications systems in transit environments, such as train control systems and fare collection systems.

Table 2 provides additional examples of industry standards and key practice documents, as they relate to threats identified by domestic passenger rail stakeholders we interviewed.

[56]The Association of American Railroads develops standards and recommended practices for the freight rail industry that also apply to Amtrak. TSA coordinates with the Association and industry officials through the industry-led Rail Security Working Committee and the Rail Information Security Committee to develop strategies, policies, and security action items, among other things.

Table 2: Examples of Threats Identified by Domestic Passenger Rail Stakeholders and Related Available Industry Standards and Key Practice Documents

Type of Threat	Standard or key practice document	Summary
Improvised explosive device	American Public Transportation Association (APTA) White Paper: Random Inspections of Carry-On Items in Transit Systems	Provides information, including legal considerations, for developing and implementing carry-on screening programs to detect explosives.
	APTA Recommended Practice: Recognizing and Responding to Unattended Packages, Objects and Baggage	Provides broad guidelines for recognizing and responding to unattended items. Generally, anything that is hidden, obviously suspicious, and not typical should be deemed suspicious.
	APTA White Paper: Trash and Recycling Receptacles for Transit Facilities	Provides guidance on the selection, design, and placement of trash and recycling receptacles to reduce risk from explosions–including the use of blast-resistant and non-blast-resistant receptacles.
Vehicle ramming	APTA Recommended Practice: Anti-Vehicle Barriers for Public Transit	Describes the types of available barriers and considerations for barrier selection and placement, such as how to counter the effects of vehicle momentum if the site to be protected is located downhill.
Cyberattack	APTA Recommended Practice: Cybersecurity Considerations for Public Transit	Overview of cybersecurity considerations that addresses threat and risk management, identifies four domains of cybersecurity, and discusses system contingency planning and resiliency.[a]
	APTA Recommended Practice: Enterprise Cybersecurity Training and Awareness	Includes a sample presentation to help secure support for a basic cybersecurity training and awareness program which highlights risk and factors for a successful program.
	Association of American Railroads: Cyber Security Effective Practices for Information Technology Procurements	Compilation of effective practices to inform industry interactions with railroad technology suppliers, including access control, password policies, and malware detection and protection.
General security	APTA Standard: Security Program Considerations for Public Transit	Overview of infrastructure security that recommends a system-wide risk assessment and identifies four pillars of security for transit security programs.[b] Recommends designating different zones of authorized access within the system, with security measures to deter, detect, and/or delay access to more secure zones.

Source: GAO analysis of available industry passenger rail security documents. | GAO-20-404

Note: The table above reflects examples of standards or key practice documents and is not intended to be an exhaustive list. Other agencies, governments, or associations may offer a variety of information and resources, which may or may not be considered key practices.

[a]APTA identifies four domains or key pillars of cybersecurity. These include information technology infrastructure, operations (policies, procedures, and processes for implementing cybersecurity plans), people (building a culture of awareness), and facilities (protecting physical hardware).

[b]APTA's four pillars of infrastructure security include: planning for potential events or incidents; operations (guidance in the form of protocols or policies); physical security protections that help manage entry to an agency's properties; and equipment and technology protections (both hardware and software related).

In addition to working with industry through APTA to develop standards and practices, TSA officials stated that the Surface Transportation Security Advisory Committee, which was established in 2019 to provide advice and recommendations to the TSA Administrator on transportation security matters, may serve as a mechanism for discussing or recommending key practices as the Committee develops.[57] Officials noted that the Committee, which includes industry and community groups, could serve as a source for identifying forward looking best practices for rail security. The Committee held initial meetings in July 2019, October 2019, and January 2020, and proposed establishing subcommittees on topics such as cybersecurity and insider threats.

None of the seven domestic rail agencies we contacted identified any security areas in which they felt recommended practices were missing. Officials from five agencies specifically commented on the usefulness of APTA publications. Officials from three agencies however, noted that many transit and rail agencies are still in the early stages of starting a cybersecurity program and that cybersecurity recommended practices are generally targeted at those agencies, as compared to agencies that already have a more sophisticated approach to cybersecurity. Officials from one agency further noted that publications related to the more technical aspects of cybersecurity (such as industrial control systems) can become outdated quickly as industry outpaces the development of security standards. TSA, CISA, and passenger rail agency officials we interviewed identified the NIST Cybersecurity Framework as the primary key practices document they reference for cybersecurity.

Domestic and foreign rail agency, and industry association officials, as well as academic experts we interviewed noted that the possibility or likelihood of a cyberattack causing physical damage or harm to rail passengers or infrastructure is unlikely and largely hypothetical at this time. Academic experts we interviewed pointed to an incident in Poland in 2008 as one of the few, if only, known incidents in which a cyber-related attack on rail resulted in physical harm. In this incident, according to news reports, a Polish teenager modified a television remote control so that it

[57]The Committee was established under the TSA Modernization Act (as part of the FAA Reauthorization Act of 2018) to provide advice and recommendations to the TSA administrator on transportation security matters. Pub. L. No. 115-254, § 1969, 132 Stat. 3186, 3609. The committee has 37 voting members representing mass transit and passenger rail, freight rail, pipelines, highway and motor transportation, and community groups.

could be used to control signals and switch points in a local tram system. Four vehicles derailed and 12 people were injured in the incident.

Several rail agency officials and stakeholders we spoke with noted that successfully hacking into train control systems would require a highly sophisticated knowledge of the system. Officials further noted that train systems are designed to fail to safe mode and stop a train in the event of an abnormal signal, and that train operators have the ability to take over controls and manually stop trains if necessary. Officials from three rail agencies, however, stated that as agencies continue to adopt new technologies and systems become more interconnected, the potential for a cyberattack increases. Additionally, CISA officials and officials from one rail agency stated that, despite the lack of many incidents to date, protecting control systems is critical given the potential catastrophic impact of a successful attack.

TSA Identifies Foreign Standards and Key Practices through Multilateral Working Groups and Bilateral Relationships, but Provides Limited Guidance to TSARs on Engaging with Foreign Rail Stakeholders

According to TSA officials, TSA identifies foreign passenger rail security standards and key practices through engagement in multilateral groups and by leveraging bilateral relationships. Examples of multilateral groups include the International Working Group on Land Transport Security and the European Association of Railway Police Forces (RAILPOL). The working group, established in 2006, consists of 19 member states, including the United States.[58] It is intended as a framework for members to openly share best practices, exchange information, and contribute to the development of surface transportation security initiatives. For example, TSA and members of the working group developed a searchable database of international surface transportation security measures (known as the SMARTbox) as a resource for surface transportation professionals to gain insights into security practices used by their peers.[59] RAILPOL, founded in 2004, is an international association of government railway police organizations. It has 22 members, including TSA and the Amtrak Police Department. Information about intermodal stations and cybersecurity can be identified and exchanged through both of these mechanisms. For example, representatives from the United Kingdom delivered a presentation on securing intermodal stations at a 2016 working group meeting, and both

[58]The working group also includes four additional observer nations.

[59]The SMARTbox contains over 350 security measures and, according to TSA officials, is currently housed on the Homeland Security Information Network. The Homeland Security Information Network is DHS' official system for sharing sensitive but unclassified information between federal, state, local, territorial, tribal, international, and private sector partners.

working group and RAILPOL meetings have included cybersecurity discussions.

Figure 3 provides an image of St. Pancras International Station in London, an intermodal station where international, local, and long distance trains converge with the London Underground.

Figure 3: St. Pancras International Station in London

Source: GAO. | GAO-20-404

Note: St. Pancras International Station is an intermodal station where international, local, and long distance trains converge with the London Underground.

Regarding bilateral engagement, TSA identifies foreign rail security standards and practices through one-on-one relationships with other countries. TSA officials noted that their level of engagement with other countries can depend on a variety of factors, including how much the countries have in common regarding transportation systems and threats, and whether or not there are formal agreements in place that allow for regular, detailed information sharing. While some relationships are ongoing, officials stated that TSA interactions with other countries are often situational or transactional—countries may reach out either directly

to TSA or through the TSAR for information about a specific issue, such as perimeter protection for surface transportation. For example:

- TSA holds biannual meetings with Transport Canada, the Canadian government department responsible for transportation policies and programs. Discussion topics from the meetings in 2017 and 2018 included Canadian efforts to develop passenger rail regulations, results from TSA derailment device testing,[60] and opportunities for collaboration.
- According to TSA officials, TSARs in several countries have facilitated engagement with foreign surface transportation officials, including passenger rail officials. For example, officials stated that one TSAR facilitated the use of TSA's Exercise Information System for an exercise on the metro system in a foreign city, as well as joint rail security training at TSA facilities in the United States. Officials further noted that another TSAR has taken initiative to facilitate quarterly meetings between foreign government and TSA surface transportation officials, including research and development and passenger rail officials.
- In addition to quarterly meetings facilitated by the TSAR, TSA officials stated that they are in regular contact with research and development officials in one country to share testing information, such as the results of derailment device testing and explosives testing on railcars, and to discuss security issues related to unmanned aircraft systems.
- TSA officials also reported that representatives attended an APTA-sponsored study trip to Brussels and London after the 2016 and 2017 rail attacks in those cities, in part, to observe lessons learned from the attacks.

Foreign governments and international rail associations also produce a variety of passenger rail security standards and key practice documents. Table 3 below provides examples of these documents and the types of threats they address.

[60]In 2017, the Al Qaeda affiliated *Inspire* magazine released an issue featuring instructions for derailing trains. TSA officials stated that they conducted a series of tests to determine whether or not the methods described in the magazine could result in derailment. In addition to sharing the results directly with one country, TSA also provided an unclassified briefing to RAILPOL counter terrorism working group members in 2018.

Table 3: Examples of Foreign Passenger Rail Security Standards and Key Practice Documents

Type of Threat	Key practice document	Summary
Improvised explosive device	British Standards Institution Publicly Available Specification 127:2014: Checkpoint Security Screening of People and their Belongings-Guide	Provides guidance for checkpoint security screening of people and their possessions, including screening location selection strategies and screening methods.
Vehicle ramming	British Standards Institution Publicly Available Specification 69:2013: Guidance for the Selection, Installation and Use of Vehicle Security Barrier Systems	Provides guidance on types of vehicle security barriers, site assessment, and barrier implementation. The document covers issues concerning vehicle restraint measures, vehicle access control, and a procurement strategy.
Cyberattack	International Association of Public Transport: Action Points: Cyber Security in Public Transport	Identifies three domains of cybersecurity and provides recommendations for, among other things, system configuration, malware prevention, and incident management.[a]
	United Kingdom Department for Transport: Rail Cyber Security: Guidance for Industry	Provides a high-level approach intended to help the rail industry reduce vulnerability to cyberattack. For example, recommends identifying all components that need patches or updates, and recommends separating networks used for train control and signals from networks passengers may use. Encourages the use of the U.S. National Institute of Standards and Technology Cybersecurity Framework in UK companies that operate critical infrastructure.
	German Federal Office for Information Security Recommendation: IT in Production. Industrial Control System Security: Top 10 Threats and Countermeasures 2019	Presents the top threats with the highest criticality for industrial control systems and options to minimize residual risk and counter these threats through methods such as network isolation, software patching, and training programs.[b]
General security	International Union of Railways: Station Security for Station Businesses. Handbook on Effective Solutions	Provides an overview of station security measures, including access control gates, cameras, visible security presence, and security considerations for design and construction.
	United Kingdom Department for Transport: Light Rail Security Recommended Best Practice	Developed to help operators devise and maintain a range of best practice security measures, including those related to the security culture of the organization, securing rail cars and stations, and securing depots and maintenance facilities.

Source: GAO analysis of available international passenger rail security documents. | GAO-20-404

[a]The International Association of Public Transport identifies three domains or key pillars of cybersecurity. These include people, policies and procedures, and physical protection.

[b]Industrial control systems are used to control industrial processes such as manufacturing, product handling, production, and distribution. They may also include transportation and passenger rail systems. These systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes.

TSA officials noted that while multilateral forums provide valuable opportunities to communicate with other countries about evolving threats, emerging security technologies, and potential key practices, interest in

forums such as the International Working Group on Land Transport Security has been in decline. For example, while the working group charter calls for annual meetings and quarterly conference calls, the full group has not met since 2016.[61] TSA and foreign government officials we spoke with stated that interest in the working group may be in decline due to factors such as retirements of key officials and lack of engagement from certain countries. These officials also noted that, as leaders in rail security, they typically provide more information about key practices to other countries in large forums than they receive. Additionally, TSA officials noted that other countries frequently used the working group-developed SMARTbox initially, but that use declined in recent years in part due to its location on the Homeland Security Information Network because users may find it difficult to navigate. Further, eight of the 10 domestic and foreign rail agencies we interviewed said they were either unfamiliar with the application or did not use it.[62] For example, officials from one domestic agency said that there was little incentive to contribute and that they found informal networks to be more useful for sharing information. In contrast, TSA and other officials we spoke to stated that bilateral relationships with trusted partners with similar sophisticated rail operations may allow for more detailed exchanges of current and emerging key security practices.

TSA Provides Limited Guidance to TSARs on Engaging with Foreign Rail Stakeholders

TSA has provided limited guidance to TSARs on engagement with foreign passenger rail stakeholders through the TSAR Toolkit (or handbook), which states that TSARs should engage with officials involved in multiple modes of transit, including rail; however, the primary focus of the document is engagement with aviation stakeholders. TSA further provides comprehensive and specific guidance for TSAR aviation engagement as part of its foreign airport assessments and air carrier inspections, but does not do so for surface transportation.[63] As discussed above, according to TSA officials, some TSARs have taken the initiative to facilitate meetings and share testing and training information related to surface transportation, including passenger rail. Passenger rail officials we talked to in one country stated that these TSAR-led initiatives served

[61]According to TSA officials, the country scheduled to host the 2018 working group meeting declined to do so; the next full meeting is currently planned for 2020.

[62]The remaining two agencies did not comment on the SMARTbox.

[63]Through its foreign airport assessment program, TSA determines whether foreign airports that provide service to the United States are maintaining and carrying out effective security measures. See 49 U.S.C. § 44907. There is no similar regulatory requirement for rail or surface transportation.

as a valuable source of information and communication with TSA. In addition, one TSA official cited the value of discussing preliminary testing findings, as well as new guidelines on topics such as security in station designs, which address concerns about security in public spaces. These efforts, however, are dependent on the individual initiative of each TSAR and are not universal. For example, one TSAR we interviewed stated that TSA's expectations and priorities for surface transportation engagement were unclear and, as a result, he focused almost exclusively on aviation.

TSA officials stated that they have focused TSAR guidance on aviation engagement because of the agency's regulatory role in this area, which, as discussed above, includes foreign airport assessments and air carrier inspections. In lieu of detailed guidance on surface transportation, officials noted they defer to the individual TSARs on how or whether to engage foreign surface transportation stakeholders. Officials emphasized this individual approach and stated that in some countries, TSAR engagement on passenger rail security issues may be limited by legal or cultural barriers. Because rail (unlike aviation) does not directly connect to the United States in most cases, officials noted that there may be less incentive for some host countries to engage. Further, some countries may not have a rail system, or may not be as advanced in rail security policies and procedures, and therefore may be less able to offer key practices.

In November 2019, TSA officials noted that they were considering adding guidance for engaging with surface transportation officials and addressing intermodal concerns to TSAR Regional Operational Implementation Plans. According to officials, these plans provide targeted guidance to TSARs for engagement within their specific regions. As of February 2020, officials stated that draft plans for two regions (Western Hemisphere and Africa/Middle East) were under review at TSA.[64] Officials further stated that these drafts, and drafts for the remaining regions currently in development, would include surface transportation-related guidance. TSA officials stated that they hoped to complete all regions' plans by the end of calendar year 2020, but they did not provide documentation for us to verify that the final plans would contain surface transportation guidance for TSARs.

The 2018 TSA Administrator's Intent document includes a goal to promote security partnerships across surface transportation systems by,

[64]The remaining two regions are Europe and Asia Pacific.

in part, identifying and communicating best practices and lessons learned to stakeholders and international partners.[65] In addition, the NIPP states that officials should share actionable and relevant information across the critical infrastructure community to build awareness and enable risk informed decision making. The TSAR Toolkit further states that, even in locations without modal connections to the United States, there is still great value in establishing key points of contact who can share best practices or facilitate the exchange of information in the event of an emergency in modes of transit outside of aviation. As the primary overseas point of contact for security matters involving all modes of transportation, TSARs are responsible for developing bilateral relationships and facilitating information sharing with foreign stakeholders, among other things.

Further leveraging formal or informal bilateral relationships could allow TSA to obtain additional passenger rail security information. While several TSARs have individually taken initiative with regard to rail, without additional guidance from TSA, there is no assurance that they will engage in these exchanges with modes outside of aviation. As a result, TSA is less likely to be fully aware of key passenger rail security practices in other countries, such as those listed in table 3 above, among others. Moreover, specific guidance will also provide TSARs with clear expectations for engaging with stakeholders, and provide TSA with greater assurance that they are engaging in a consistent manner. TSA's new Regional Operational Implementation Plans provide an opportunity for TSA to more clearly incorporate targeted guidance to encourage TSAR outreach and information sharing in specific areas.[66] Recent efforts by TSARs in several countries demonstrate practices, such as opening lines of regular communication on surface transportation, including passenger rail, which could be replicated in other countries.

[65]Transportation Security Administration, *Administrator's Intent*, (June 1, 2018). This document is intended to identify how TSA will execute the 2018-2026 TSA Strategy through 2020.

[66]While TSARs are based in one country, they are typically responsible for one or more countries in a specific region.

TSA Uses Various Mechanisms to Share Security Standards and Key Practices but Does Not Fully Incorporate NIST Cybersecurity Standards in the BASE

TSA Shares Information about Standards and Key Practices through Its Participation in Working Groups, and through Assessments and Exercises

According to TSA officials and domestic rail stakeholders we interviewed, TSA uses various mechanisms such as the Transit Policing and Security Peer Advisory Group, monthly conference calls with rail stakeholders,[67] and the annual APTA roundtable meeting to share and discuss a range of security information with stakeholders, including information about standards and key practices.[68] These mechanisms provide opportunities to discuss issues related to intermodal stations and cybersecurity key practices.

TSA also shares information about key practices with domestic stakeholders through voluntary TSA programs such as BASE, the Intermodal Security Training and Exercise Program,[69] and the Visible

[67]According to TSA officials, TSA's Intelligence and Analysis Office shares information about current threats and other topics during monthly classified calls and also holds periodic meetings with industry members in response to imminent threats.

[68]We have previously reported that federal agencies use a variety of mechanisms to implement collaborative efforts, and that these mechanisms can be used for multiple purposes, including information sharing and communication. Mechanisms can include national strategies, interagency groups, conferences and communities of practice, and collaboration technologies such as shared databases and web portals, among others. We also identified key issues to consider when implementing interagency collaborative mechanisms. See GAO, *Managing for Results: Key Considerations for Implementing Interagency Collaborative Mechanisms,* GAO-12-1022 (Washington, D.C.: Sep. 27, 2012).

[69]The Intermodal Security Training and Exercise Program is a voluntary program involving multi-jurisdictional activities ranging from seminars to full-scale exercises. The exercises are conducted across surface transportation modes and are intended to enhance security preparedness and incident management skills, as well as share lessons learned and best practices, among other things.

Intermodal Prevention and Response program.[70] TSA officials provided information about how they incorporate information from foreign threats and attacks into these programs. Specifically:

- TSA officials noted that TSA initially developed the BASE program around standards that were produced by APTA and other industry partners following the 2004 terrorist attacks on commuter trains in Madrid and the 2005 terrorist attacks on the London subway system. According to TSA officials, the APTA standards and recommended practices, which evolve based on threats and lessons learned, form the basis for the BASE assessment template. One way in which TSA helps communicates these standards and practices to agencies is through the questions in the template. Officials noted that lessons learned from foreign rail security incidents have been used to further support certain security concepts in the BASE, such as assessment questions related to whether agencies engage in public outreach for security awareness (e.g. “If You See Something, Say Something”) and report suspicious activity.
- TSA officials reported that they consider overseas and domestic attack methods and tactics when planning Intermodal Security Training and Exercise Program exercises to raise awareness of emerging tactics and threats. These exercises are intended to share best practices and lessons learned, among other things. Officials noted that they recently incorporated cyber, chemical, and vehicle-ramming attacks into the program’s objectives based on recent domestic and overseas incidents, and that they shared resources, information, and best practices for security solutions. For example, officials reported conducting two regional exercises that focused on chemical threat elements as the result of a 2017 plot in Australia.[71]

[70]TSA deploys teams to conduct Visible Intermodal Prevention and Response operations as a way to augment the security of, and promote confidence in, surface transportation systems. Deployments can include random bag searches and high-visibility patrols at passenger rail systems.

[71]In August 2017, investigators in Australia reported that suspects were working with Islamic State operatives to create an improvised chemical device and detonate it in a public area.

TSA further reported hosting a series of vehicle ramming program workshops in the wake of attacks in New York City and Europe.[72]

- According to TSA officials, TSA has not made any recent changes to the Visible Intermodal Prevention and Response program directly as a result of lessons learned or key practices resulting from a foreign rail security incident; however, officials said they regularly integrate information about foreign incidents and threats when planning program deployments. Officials also noted that the majority of current deployments are for surface transportation, which includes rail.[73]

Regarding cybersecurity, TSA has shared information about cybersecurity key practices, including the NIST Cybersecurity Framework, through a series of regional cybersecurity Intermodal Security Training and Exercise Program workshops since 2017.[74] These "5N5" workshops listed five nontechnical cybersecurity actions an agency could take in 5 days, including: (1) develop familiarity with the NIST Cybersecurity Framework; (2) implement a unique password change policy; (3) understand the latest phishing and spam trends and how to message awareness; (4) differentiate access control among staff; and (5) report cybersecurity incidents.

Six of the seven domestic rail agencies we spoke with were generally satisfied with TSA's efforts to share security and key practice information;[75] however officials from two of these six agencies also expressed concerns about timeliness and quality of cybersecurity

[72]In October 2017, an individual used a commercial-grade rental truck to attack pedestrians on a bike path in New York City. In March 2017, a rental car was used to attack pedestrians on Westminster Bridge in London, England. In July 2016, an individual used a rental truck to attack pedestrians in Nice, France. While none of these incidents directly involved passenger rail, officials from three domestic rail agencies we spoke to cited vehicle rammings or the use of a vehicle as a weapon as a threat to passenger rail.

[73]In 2005, we recommended that TSA evaluate the applicability and potential benefits of implementing certain practices we observed overseas, including covert testing and random passenger screening. In 2009, in response to this recommendation, TSA reported that it was reviewing options to expand covert testing into exercises in the mass transit and passenger rail environment and identified the Intermodal Security Training and Exercise Program as a venue where covert testing could be appropriate in assessing the effectiveness of security activities and measures. TSA also reported exploring opportunities to integrate covert testing periodically to assess the effectiveness of Visible Intermodal Prevention and Response teams. See GAO-05-851.

[74]TSA officials reported that, as of October 2019, TSA had conducted 16 cybersecurity workshops.

[75]One agency did not comment on TSA's information sharing efforts.

information provided by TSA. For example, officials from one agency stated that they received limited cybersecurity information from TSA and that the information they did receive was of limited use because it was targeted at agencies without a sophisticated cybersecurity program. An official from another agency noted that while there were opportunities to discuss cybersecurity, the information provided was often general in nature and there was limited time for discussion in certain mechanisms because of the large number of people involved. This official also noted that while the information TSA provides is valuable and there are mechanisms available to share information about a range topics, discussions are typically related to security incidents and threats, as opposed to key practices.

TSA officials acknowledged that the agency's cybersecurity efforts were still in the early stages. They further noted that the implementation plan for the 2018 Cybersecurity Roadmap, which, among things, calls for improving information sharing and partnering with stakeholders to promote the adoption of best practices and industry and/or international standards, was only recently signed in September 2019.

In addition to TSA's information sharing mechanisms, domestic rail agency officials we spoke to reported learning about foreign key practices through personal experience and direct engagement with foreign rail counterparts. For example, officials from two agencies we spoke to hosted visits from foreign rail officials to study security measures, among other things. Officials from one agency noted they provided information to Hong Kong through APTA on key practices for managing large protest crowds in an urban transit environment. Officials from another agency noted that they participate in international information sharing surveys and research to learn about cybersecurity practices by foreign rail operators, and sent representatives to an international mass transit training forum on the development of threat, vulnerability, and risk assessments.

Domestic rail agencies also identified several changes they have made to their physical security systems as a result of key practices or lessons

learned from foreign rail incidents.[76] For example: increasing random patrols and high visibility deployments of security officers, changing security camera placement to better capture station exits, and increasing security awareness messaging to employees and passengers.[77] Additionally, officials from one agency noted that they revised subway evacuation plans to direct people towards areas less vulnerable to an attack after reviewing lessons learned from recent vehicle-based attacks in Europe. With regard to cybersecurity, one domestic agency we spoke to noted that recent wide-spread global cyberattacks reinforced challenges they have securing legacy Information Technology systems against threats such as ransomware threats. As a result, the agency is focused on identifying expiring technologies and replacing those that can no longer be patched or updated. Officials from another agency noted that they have increased the number of firewalls they use to further segment and protect systems.

Table 4 below provides information on mechanisms that can be used to identify and share rail security key practice information, as identified by TSA and domestic stakeholders.

[76]In 2005, we reported that certain security practices used overseas could pose political, legal, fiscal, and cultural challenges in the United States, where residents may not be as willing to accept more intrusive security measures. See GAO-05-851. TSA officials we interviewed for this review stated that this remains the case today. For example, officials cited 'red team' practices in one country that involve live, simulated terrorist events in which neither the transit workers or the public are aware that the incident is a planned exercise.

[77]In 2012, we reported on lessons learned from foreign attacks that U.S. rail agencies reported incorporating into their security systems. These included enhancements to public awareness and messaging campaigns, increased use of motorized emergency response vehicles to reach victims after an attack, and reinforcement of the value of closed-circuit television for forensic investigations after an attack. See GAO-13-20.

Table 4: Mechanisms Cited by the Transportation Security Administration (TSA) or Domestic Passenger Rail Stakeholders That Can be Used to Identify and Share Rail Security Key Practice Information

Mechanism	Description	Physical security	Cybersecurity
American Public Transportation Association (APTA) working groups	APTA has 27 active working groups on a variety of topics, including infrastructure security, risk management, and cybersecurity. Working groups are comprised of APTA members and nonmember volunteer stakeholders, including federal partners like TSA, who represent key segments of the transportation industry. These groups develop and publish standards and best practice documents.	●	●
TSA Transit Policing and Security Peer Advisory Group	TSA established the group in 2007 as a communication and liaison group consisting of transit police chiefs and security directors from mass transit systems across North America. The group is designed to provide subject matter expertise on mass transit security-related issues. The group has 33 mass transit stakeholder members and is chaired by a transit police chief.	●	●
Annual APTA Security Roundtable	APTA hosts an annual security roundtable where APTA, TSA and other federal partners, police chiefs and security directors of APTA member organizations exchange information. TSA shares information on security threats, capability gaps, and technology with mass transit stakeholders.	●	●
TSA sponsored monthly conference calls	TSA hosts monthly information sharing teleconferences with approximately 500 rail stakeholders from the transit security community. These calls include threat briefings and discussions of issues and best practices related to mass transit and passenger rail security.	●	●
TSA Surface Transportation Security Advisory Committee	TSA established the committee in 2019 in response to the provisions of the TSA Modernization Act. The committee is composed of members representing surface transportation providers and users, including passenger rail, and non-voting members representing federal departments and agencies with surface transportation oversight. The committee is charged with advising the TSA Administrator on surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security	●	●
Public Transportation Information Sharing and Analysis Center	Managed by APTA in collaboration with TSA, this is a 24/7 center that collects, analyzes, and disseminates alerts and incident reports. The center produces daily reports developed through analysis of numerous intelligence sources.	●	●
TSA Baseline Assessment and Security Enhancement (BASE)	TSA's BASE assessment is a voluntary review in which surface inspectors evaluate the security programs of transportation entities, offer technical assistance, and share best practices. The assessment analyzes the security program for each transit system and identifies vulnerabilities. The BASE consists of 17 security action items that address, among other best practices, security training and awareness programs, cybersecurity, and access control.	●	●

Mechanism	Description	Physical security	Cybersecurity
TSA Intermodal Security Training and Exercise Program	TSA conducts multi-agency, multi-jurisdictional activities ranging from seminars to full-scale exercises. Full-scale exercises focus on implementing and analyzing plans, policies, and procedures. The voluntary exercises are conducted across surface transportation modes including passenger rail.	●	●
TSA cybersecurity workshops	In fiscal year 2017, TSA developed a series of regional surface transportation-focused cybersecurity workshops. The workshops were intended to provide an awareness of existing U.S. government cybersecurity support programs available resources and provide an opportunity for participants to share best practices.	—	●
Association of American Railroads Rail Information Security Committee	Established in 1999 to mitigate cyber risk and counter cyber threats. The group is comprised of chief information security officers and cybersecurity leads from each of the Class I freight railroads and Amtrak, among others, and is supported by the Association of American Railroads. The group develops and shares effective practices and threat, vulnerability, and incident response information.	—	●

Legend: — Not discussed in this mechanism ● Discussed in this mechanism

Source: GAO analysis. | GAO-20-404

Note: We previously reported on mechanisms eight high-volume rail agencies cited as useful in obtaining and sharing rail security information. These mechanisms included the Peer Advisory Group, the Public Transportation Information Sharing and Analysis Center, and the BASE and Intermodal Security Training and Exercise programs, among others. See GAO, Passenger Rail Security: Consistent Incident Reporting and Analysis Needed to Achieve Program Objectives, GAO-13-20 (Washington, D.C.: Dec. 19, 2012).

TSA Does Not Fully Incorporate NIST Cybersecurity Standards into Its BASE Assessments

While TSA has taken initial steps to share cybersecurity key practices and other information with passenger rail stakeholders, the BASE assessment, does not fully reflect the updated cyber key practices presented in the NIST Cybersecurity Framework, nor does it include the framework in a list of available cyber resources.[78] As discussed above, TSA uses the BASE assessment to share security best practices with transit agencies, among other things.[79] Our review of the BASE

[78]For example, as discussed above, TSA has shared cybersecurity information through APTA working groups, through training exercises such as the Intermodal Security Training and Exercise Program, and through regional cybersecurity workshops promoting the NIST Cybersecurity Framework. TSA further shares cybersecurity key practices through questions in the BASE.

[79]The cybersecurity section of the BASE template assesses the extent to which agencies have taken a series of steps to develop a comprehensive cybersecurity strategy. Specifically, it assesses the extent to which agencies have conducted a cybersecurity risk assessment; implemented protocols to ensure that all Information Technology facilities are secured; and provided training on recognizing cyber threats to all employees, among other things.

cybersecurity questions in the template found that they cover selected activities associated with three of the five functions outlined in the framework– Identify, Protect, and Respond. For example, the BASE asks agencies if they ensure training reinforces cybersecurity roles and responsibilities, which corresponds to the awareness and training category of the NIST Protect function. However, the remaining two functions—Detect and Recover—are not represented in the BASE. According to the framework, when considered together, these functions provide a high-level, strategic view of the life cycle of an organization's management of cybersecurity risk.

TSA officials stated that they regularly review the BASE and noted that the questions are intended to reflect both industry key practices and agency policy; however, they also stated that the agency has not updated the BASE cybersecurity questions since NIST released its Cybersecurity Framework in 2014.[80] In January 2020, officials responsible for the BASE acknowledged that the cybersecurity questions should be updated to reflect the framework. TSA officials also noted that they would want to align changes to the BASE cybersecurity questions with any new guidance or direction provided by the newly established Surface Transportation Security Advisory Committee. As of January 2020, the Committee is in its initial start-up phase, and has not yet provided any reports or recommendations or published a timeline or project plan. Further, because the framework functions organize basic cybersecurity activities at their highest level, incorporating elements of all five functions into the BASE template should not require additional guidance from the Committee.

The 2015 TSA *Transportation Systems Sector-Specific Plan* states that encouraging the adoption of the NIST Cybersecurity Framework across all transportation modes supports the plan's goal to manage the security risks to the physical, human, and cyber elements of critical transportation infrastructure. The plan also states that encouraging the adoption of the framework contributes to several of the NIPP's calls to action related to sharing actionable and relevant information. TSA considers the framework a best practice document.

By updating the BASE cybersecurity questions to align more closely with the core functions in the NIST Cybersecurity Framework, TSA could

[80]The NIST Cybersecurity Framework was first released in 2014, after TSA added cybersecurity questions to the BASE in 2013. The framework was updated in 2018.

better assist passenger rail and other operators in identifying current key practices and improving their cybersecurity posture. As a result, transit operators would be more aware of cybersecurity vulnerabilities and better prepared to reduce the impact from a cybersecurity incident. In addition, this would create a more consistent cybersecurity approach from TSA, since the agency promotes the framework through other mechanisms, such as the series of cybersecurity workshops, as noted above.

Conclusions

Recent physical and cyberattacks in U.S. cities and Europe demonstrate the evolving nature of the threats to passenger rail and highlight the importance of working with both domestic stakeholders and foreign rail security partners. As such, TSA actively engages with domestic passenger rail stakeholders, but could do more to engage with foreign stakeholders. TSARs stationed abroad are well positioned to further leverage bilateral relationships with foreign passenger rail stakeholders, and several TSARs have taken initiative to do so. However, TSA provides only limited guidance to TSARs on surface transportation engagement. Without specific guidance, there is no assurance that TSARs will engage in these exchanges with modes outside of aviation. TSA's new Regional Operational Implementation Plans provide an opportunity to more clearly incorporate targeted guidance to encourage TSAR outreach and information sharing in specific areas. Additionally, such guidance will provide TSA with greater assurance that TSARs are engaging with foreign stakeholders in a consistent manner.

TSA uses various mechanisms to share security standards and key practice information with rail stakeholders, including through BASE assessments. The cybersecurity questions in the BASE template, however, do not fully reflect two of the five core areas identified in the NIST Cybersecurity Framework. By updating the BASE cybersecurity questions to align more closely with current key practices such as the framework, TSA could better assist passenger rail and other operators in improving their cybersecurity posture. As a result, transit operators would be more aware of cybersecurity vulnerabilities and better prepared to reduce the impact from a cybersecurity incident.

Recommendation for Executive Action

We are making two recommendations to TSA.

The TSA Administrator should ensure that the TSAR Regional Operational Implementation Plans include guidance on how TSARs are to engage with foreign surface transportation stakeholders, including passenger rail stakeholders. (Recommendation 1)

The TSA Administrator should update the BASE cybersecurity template to ensure it reflects cybersecurity key practices, including the Detect and Recover functions outlined in the NIST Cybersecurity Framework. (Recommendation 2)

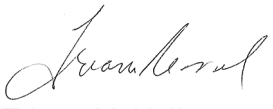
Agency Comments and Our Evaluation

We provided a draft of this report to DHS for review and comment. DHS provided written comments, which are reprinted in appendix II, and also provided technical comments, which we incorporated as appropriate.

DHS concurred with both recommendations and described actions TSA plans to take to address them. Specifically, to address recommendation 1, TSA plans to draft an Operational Implementation Plan, which will provide guidance to TSARs for engaging with foreign surface transportation stakeholders, including in passenger rail security. According to TSA, this plan will also serve as the outline for the development of Regional Operational Implementation Plans, which will help align resources worldwide. To address recommendation 2, TSA plans to update the BASE Cybersecurity Security Action Item section to ensure it reflects the NIST Cybersecurity Framework Detect and Recover functions. These actions, if fully implemented by TSA, should address the intent of both recommendations.

We are sending copies of this report to the appropriate congressional committees and the acting Secretary of Homeland Security. In addition, the report is available at no charge on the GAO website at http://www.gao.gov.

If you or your staff members have any questions about this report, please contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov. Contact points for our Office of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributors to this report are listed in appendix III.



Triana McNeil
Director, Homeland Security and Justice

List of Addressees

The Honorable Roger F. Wicker
Chairman
The Honorable Maria Cantwell
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Ron Johnson
Chairman
The Honorable Gary C. Peters
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Bennie G. Thompson
Chairman
The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Michael T. McCaul
House of Representatives

The Honorable John Katko
House of Representatives

The Honorable Bonnie Watson Coleman
House of Representatives

Appendix I: Physical Security and Cybersecurity Key Practices Cited by Domestic and Foreign Stakeholders

We asked domestic and foreign passenger rail agencies and foreign passenger rail stakeholders we interviewed to identify some security related key practices or lessons learned that they employ, including, but not limited to, intermodal stations and cybersecurity.[1] Table 5 below provides examples of common security practices both domestic and foreign officials identified; table 6 shows several additional key practices foreign rail stakeholders cited. These tables are not intended to be a comprehensive list, but provide examples of key security practices utilized by selected domestic and foreign rail agencies.

Table 5: Examples of Common Physical Security and Cybersecurity Key Practices Cited by Selected Domestic and Foreign Passenger Rail Stakeholders

Key practice	Physical security	Cybersecurity
High visibility security patrols	●	—
Canines trained to detect vapor from bomb residue	●	—
Random bag inspections and random security patrols	●	—
Security camera systems/Closed-circuit television	●	—
Public service security announcements (e.g. See Something, Say Something in the U.S. and See it, Say it, Sorted in the United Kingdom)	●	—
Employee training emphasizing security awareness[a]	●	—
Employee training emphasizing ways to tell the difference between unattended items and suspicious items[b]	●	—
Internal threat monitoring and/or risk assessments	●	—
Close partnerships with federal and state and local partners	●	—

[1]The officials we interviewed represented the following seven domestic passenger rail agencies: Amtrak; Chicago Transit Authority; Los Angeles County Metropolitan Transportation Authority; Massachusetts Bay Transportation Authority; New York City Metropolitan Transit Authority; San Francisco Bay Area Rapid Transit; and Washington Metropolitan Area Transit Authority. We also interviewed three foreign passenger rail agencies in the United Kingdom and Germany (London Underground, Deutsche Bahn, and Berliner Verkehrsbetriebe), the British Transport Police, Network Rail, and the United Kingdom's Department for Transport. One rail agency—the New York City Metropolitan Transit Authority—provided written responses to our questions.

Key practice	Physical security	Cybersecurity
Access controls to the network or to secure spaces with sensitive control and communications equipment	—	●
Vulnerability scans and/or penetration testing to test for system weaknesses	—	●
Network segmentation to isolate the effects of a potential cyberattack	—	●

Legend: — Key practice does not apply to this aspect of rail security ● Key practice applies to this aspect of rail security

Source: GAO analysis. | GAO-20-404

Note: The examples shown were provided in response to the following interview question: "What are some security related key practices or lessons learned that you employ, including, but not limited to, intermodal stations and cybersecurity?" We asked this of domestic and foreign passenger rail agencies and foreign passenger rail stakeholders we interviewed (seven domestic and six foreign). Agencies may utilize certain security practices even if they did not cite them as a key practice example during our interviews. The table above is not intended to be a comprehensive list. We did not evaluate the appropriateness or effectiveness of the practices identified.

[a]The type of awareness training varied in the foreign agencies we interviewed. For example, in the United Kingdom, officials stated that all employees are trained to take an active role in security and to actively engage customers and report suspicious incidents. In contrast, German officials said that public service employees are not expected to take an active role in security beyond awareness. They noted it would not be culturally acceptable for non-security employees to play an active security role.

[b]Rail employees in the UK are encouraged to use the H-O-T method to examine an attended item. H = is it hidden; O = is it obviously suspicious; and T = is it typical of what you would expect to find in the location.

Table 6: Additional Security Key Practices Cited by Selected Foreign Passenger Rail Stakeholders

Key Practice	Physical security	Cybersecurity
Project Servator (combines high visibility, random patrols, behavior detection, public awareness, and customer service)	●	—
Behavior detection[a]	●	—
Aviation-style security screening[b]	●	—
Bollards or other physical barriers around station perimeters and open spaces[c]	●	—

Legend: — Key practice does not apply to this aspect of rail security ● Key practice applies to this aspect of rail security

Source: GAO analysis. | GAO-20-404

Note: The examples shown were provided in response to the following interview question: "What are some security related key practices or lessons learned that you employ, including, but not limited to, intermodal stations and cybersecurity?" We asked this of domestic and foreign passenger rail agencies and foreign passenger rail stakeholders we interviewed (seven domestic and six foreign). Domestic agencies may utilize certain security practices even if they did not cite them as a key practice example during our interviews. Additionally, some practices may not be applicable to all

passenger rail agencies. For example, it is difficult to incorporate aviation-style security screening in subway systems due to factors such as the high volume of passengers and multiple access points.

[a]In the United Kingdom, officials we talked to placed an emphasis on the use of behavior detection techniques in security patrols. Employees are encouraged to apply the W-H-A-T protocol to evaluate behavior: W = What are they doing; H = How are they behaving; A = Alone or acting with others; T = Threat – what Type do they pose?

[b]Passengers travelling internationally via the Eurostar train line (between London and European cities such as Paris and Brussels) undergo security screening similar to aviation screening, such as bag screening and passing through metal detectors. Unlike airline travel, the volume of liquid a passenger may carry is not restricted.

[c]United Kingdom officials stated that regulations require certain categories of stations (e.g. those with high passenger volume and historic or cultural significance) to install bollards or other physical barriers in part to protect against vehicle attacks. According to officials we interviewed, Germany does not require bollards or physical barriers around any stations. In the U.S., anti-vehicle barriers are an American Public Transportation Association recommend practice, but are not required.

Figure 4 below shows an example of a Project Servator poster displayed during an exercise at St. Pancras International Station in London. As noted in table 6 above, foreign passenger rail stakeholders cited Project Servator as a key rail security practice.

Figure 4: Project Servator Poster Displayed During an Exercise at St. Pancras International Station in London

Source: GAO. | GAO-20-404

Appendix II: Comments from the U.S. Department of Homeland Security

U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

March 26, 2020

Ms. Triana McNeil
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

RE: Management's Response to Draft Report GAO-20-404, "PASSENGER RAIL SECURITY: TSA Engages with Stakeholders but Could Better Identify and Share Standards and Key Practices"

Dear Ms. McNeil:

Thank you for the opportunity to comment on this draft report. The U.S. Department of Homeland Security (DHS or the Department) appreciates the U.S. Government Accountability Office's (GAO) work in planning and conducting its review and issuing this report.

The Department is pleased to note GAO's recognition of the Transportation Security Administration's (TSA) ongoing efforts to leverage industry partnerships to reduce risk across all sectors of surface transportation. As a leader in the transportation security network, TSA continuously works to raise the global baseline of aviation and surface transportation security. However, securing the transportation system is a complex task, and TSA cannot do it alone. TSA is committed to maintaining the strong partnerships across governments, industry, and with others that are integral to success in this shared security mission.

The draft report contained two recommendations, with which the Department concurs. Attached find our detailed response to each recommendation. DHS previously submitted technical comments under a separate cover for GAO's consideration.

Again, thank you for the opportunity to review and comment on this draft report. Please feel free to contact me if you have any questions. We look forward to working with you again in the future.

Sincerely,

JIM H CRUMPACKER

Digitally signed by JIM H CRUMPACKER
Date: 2020.03.26 11:17:00 -04'00'

JIM H. CRUMPACKER, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

Attachment: Management Response to Recommendations Contained in GAO-20-404

GAO recommended that the TSA Administrator:

Recommendation 1: Ensure that the TSAR [TSA Representative] Regional Operational Implementation Plans include guidance on how TSARs are to engage with foreign surface transportation stakeholders, including passenger rail stakeholders.

Response: Concur. The TSA International Operations (IO) office is drafting an Operational Implementation Plan (OIP) that will establish IO's operational efforts, including with regard to surface transportation security. Through the OIP's objectives and milestones, IO will directly support the 2018-2026 TSA Strategy, as well as the DHS International Engagement Strategy. Specifically, the OIP will provide guidance to TSARs for engaging with foreign surface transportation stakeholders in surface transportation, including passenger rail security. The OIP will also serve as the outline for the development of Regional OIPs, which will help align resources appropriately worldwide. Estimated Completion Date (ECD): September 30, 2020.

Recommendation 2: Update the BASE [Baseline Assessment for Security Enhancement] cybersecurity template to ensure it reflects cybersecurity key practices, including the Detect and Recover functions outlined in the NIST [National Institute of Standards and Technology] Cybersecurity Framework.

Response: Concur. The TSA Surface Operations office is working with TSA's Policy, Plans, and Engagement personnel to update the BASE Cybersecurity Security Action Item section. The template will be reviewed to ensure the question set and/or guidance reflect the NIST Cybersecurity Framework functions of Detection and Recovery. ECD: September 30, 2020.

3

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Triana McNeil (202) 512-8777 or McNeilT@gao.gov

Staff Acknowledgments

In additional to the contact named above, Christopher Ferencik (Assistant Director), Sarah Turpin (Analyst in Charge), Chuck Bausell, Benjamin Crossley, Suzanne Kaasa, Tracey King, Ronald La Due Lake, William Reed, and Adam Vogt made key contributions to this report.