Protecting Public Areas

Best Practices and Recommendations

October 2019

Transportation Security Administration

Background

In mid-September 2016, a group of industry, government, academic, international, and public officials gathered at TSA Headquarters in response to the atrocities at Brussels International Airport and Istanbul Ataturk Airport. This working group continued to meet between 2016 and 2018 to explore how to address and respond to the evolving tactics and techniques that adversaries are employing to attack civilian targets in public areas, and was tasked with devising a strategy to share information, prevent attacks, and protect infrastructure from emerging threats to public spaces of transportation venues. The threat against public areas of transportation venues was further amplified after the 2017 attack at Ft. Lauderdale International Airport.

Based on persistent threats, the group thoroughly evaluated security measures, gaps, and needs within aviation and surface modes of transportation to begin the development of a national-level framework to secure public areas. Input from international partners in the United Kingdom, Europe, and Israel on lessons learned also contributed to the formulation of these best practices.

Several sub-working groups were established to support various work streams to develop these security best practices, including: Threat, Risk, and Intelligence; Education and Training; Meta Leadership; Building Design and Infrastructure; Public Area Detection Resources; Insider Threat; Law Enforcement; and Resumption of Trade. Collectively, the recommendations were presented to enhance security in public spaces at airports and throughout the transportation system. Not all recommendations apply to all operating environments; rather they are intended to serve as options operators can select based on their unique circumstances. Consequently, the Public Area Security National Framework was published in May 2017, encompassing the aforementioned recommendations referred to as Public Area Security Best Practices.

In response to the enactment of the *TSA Modernization Act* (the Act) (Division K, Title I of the *Federal Aviation Administration (FAA) Reauthorization Act of 2018* (P.L. 115-254; 132 Stat. 3186; October 5, 2018) and the requirements in Section 1931(c)(2) of the Act related to the security of public areas, TSA looked to build upon the valuable work that was already accomplished between 2016-2018. This document is being issued in response to 1931 (c) (2) which states "(2) BEST PRACTICES.—Not later than 1 year after the date of enactment of this Act, and periodically thereafter, the Secretary shall publish on the Department website and widely disseminate, as appropriate, current best practices for protecting and enhancing the resilience of public areas of transportation facilities (including facilities that are surface transportation assets), including associated frameworks or templates for implementation."

TSA, in coordination with the Cybersecurity and Infrastructure Security Agency (CISA), invited public and private stakeholders from both aviation and surface entities to reconvene and become part of a newly established working group to collaborate and develop updated non-binding recommendations for enhancing security in public areas of transportation facilities. It is important to note that the recommended best practices are voluntary and not mandates to transportation entities. The working group consisted of key stakeholders from airline, airport, air cargo, and general aviation associations as well as stakeholders from mass transit and passenger rail and highway motor carrier. The following reflects the work of this group, which convened several times in 2019 to provide input, updates, and edits to the existing public area security best

practices recommendations, as well as provide additional best practices and identify current challenges.

Public Areas Security Best Practices

Information Sharing

During an incident, time is precious and a large-scale response to an incident involves multiple agencies with law enforcement playing a critical role in the preservation of security in the public area. Time coupled with detailed, accurate and expeditious information sharing is critical. The 'golden hour' is used in emergency medicine to describe how and when an individual receives medical care within the first hour of a traumatic injury. Immediate treatment significantly increases the likelihood of survival. For mass casualty incident responses, officials have the 'platinum ten minutes' to determine communications strategies, share information, and formulate a mitigation strategy. When responding to an incident, agencies must be able to communicate effectively with each other in order to relay updates and prevent duplicative work. Relationships that recognize and utilize the capabilities and responsibilities for any first responder, vendor, or party who can be integrated into a response will save time and prevent confusion.

Recommendation 1: Cultivate Relationships

Transportation system owners and operators should initiate discussions with relevant state, local, tribal, territorial, military and federal law enforcement personnel to cultivate relationships and proactively identify roles and responsibilities in the event of an incident. Transportation venues should incorporate other first responders to train, conduct exercises and address planning for all aspects of incident response. Additionally, transportation venues should maintain relationships with emergency medical services personnel, as they may be needed for immediate treatment of injured persons. Finally, responsible federal, state, local, territorial and tribal agencies should consider developing notification procedures, building relationships, and consequently trust, with local community partners, as they can offer insight and timely information in the event of an incident.

The same relationship principles apply to critical infrastructure. Given the diverse authorities, roles, and responsibilities of critical infrastructure partners, a proactive and inclusive partnership among all levels of government and the private and non-profit sectors provides optimal critical infrastructure security and resilience. The National Infrastructure Protection Plan (NIPP 2013: *Partnering for Critical Infrastructure Security and Resilience*) describes a national unity of effort to achieve critical infrastructure security and resilience.

Recommendation 2: Develop Communication Strategies to Enhance Information Exchanges

When responding to an incident, incident commanders and involved parties should monitor the flow of information to maximize the proactive relay of real-time and accurate alerts to other first responders, appropriate industry partners and the public while minimizing or preventing the

transmission of inaccurate information whether it be purposefully by an adversary or unintentionally by an observer. This should include communication with affected community members—infrastructure owners and employees, who may not have a response role, but may have information regarding the situation and will also have their own communication responsibilities and requirements. Incident commanders should consider utilizing mass notification systems like the Federal Emergency Management Agency's (FEMA) Integrated Public Alert and Warning System (IPAWS), as well as social media platforms to disseminate information to transportation community employees, travelers, and the general public. Communications strategies should avoid solely relying on cellular networks, as they can easily be overrun in times of emergency, and should consider employing FirstNet as applicable**.**

FirstNet provides public safety officials with streamlined and interoperable communications to execute their missions while working with other public safety officials at all levels of government. FirstNet offers priority and preemption capabilities and coverage solutions for public safety communications, allowing public safety officials to avoid network congestion that occurs during emergencies. When sharing information, venues should always consider the sensitivity of the content. Venues should prepare and have plans or Standard Operating Procedures in case of an emergency event and generic incident-related announcements in advance of an event to save time and resources. Finally, personnel who communicate via radio should consider purchasing equipment capable of transmitting messages on multiple frequencies, and coordinate in advance with partners to ensure communications equipment is compatible, and to establish a common channel(s) for communications.

Another noteworthy resource to effectively share information is the Homeland Security Information Network (HSIN). HSIN is the trusted network for homeland security mission operations to share sensitive but unclassified information. Federal, state, local, territorial, tribal, international and private sector homeland security partners use HSIN to manage operations, analyze data, send alerts and notices, and share the information they need to do their jobs and help keep their communities safe. The Critical Infrastructure community on HSIN (HSIN-CI) is the primary system through which private sector owners and operators, the Department of Homeland Security (DHS), and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure. HSIN-CI provides real-time collaboration tools including a virtual meeting space, document sharing, alerts, and instant messaging at no charge.

SAFECOM was formed in 2001 after the terrorist attacks of September 11, 2001 as part of the Presidential E-Government Initiative to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters. SAFECOM's mission is to improve designated emergency response providers' inter-jurisdictional and inter-disciplinary emergency communications interoperability through collaboration with emergency responders across Federal, State, local, tribal, and territorial governments, and international borders.

FirstNet https://www.firstnet.gov

https://www.dhs.gov/homeland-security-information-network-hsin

DHS SAFECOM https://www.dhs.gov/safecom/resources

Recommendation 3: Enhance Situational Awareness

Having an effective peer-to-peer information sharing network—that enhances situational awareness on threats to transportation networks—is key to strengthening public area security across the transportation sector. DHS has worked for many years to further enhance situational awareness by developing systems and products such as the National Terrorism Advisory System (NTAS), the CISA Security of Soft Targets and Crowded Places–Resource Guide (April 2019), the DHS Soft Targets and Crowded Places Security Plan Overview (May 2018), the CISA Active Shooter Preparedness, DHS Run/Hide/Fight Pocket Cards, the United States Secret Service 2018 Mass Attacks in Public Spaces Report, CISA Cybersecurity and the DHS Countering Unmanned Aircraft Systems (UAS) Legal Authorities fact sheet.

https://www.dhs.gov/national-terrorism-advisory-system

Security of Soft Targets and Crowded Places Resource Guide

Soft Targets and Crowded Places Security Plan Overview

Active Shooter Human Resources or Security Professional

Run/Hide/Fight Pocket Cards
https://www.dhs.gov/sites/default/files/publications/active_shooter_pocket_card_508.pdf

https://www.secretservice.gov/data/press/reports/USSS_FY2019_MAPS.pdf

CISA Cybersecurity https://www.dhs.gov/cisa/cybersecurity

UAS https://www.dhs.gov/cisa/uas-critical-infrastructure

Over the years, TSA has significantly increased face-to-face industry engagement, produced numerous intelligence products and supported the dissemination of additional products from our Intelligence Community partners. TSA will continue to disseminate Security Awareness Messages (SAM), Transportation Intelligence Notes (TIN), tear-lines, and related intelligence products to its transportation stakeholders. The agency will continue to facilitate classified briefings with both aviation and other transportation sector stakeholders.

These efforts include, in conjunction with the Office of the Director of National Intelligence and industry partners, creation and operationalizing of the Aviation Domain Intelligence Integration & Analysis Cell (ADIAC) in 2016 to enhance government and industry two-way aviation security information sharing on threat awareness. Through the ADIAC, professionals from government and industry come together physically and virtually to share sensitive and classified information in their common pursuit of aviation security.

Additionally, TSA continues to fund the American Public Transportation Association's (APTA)

Public Transportation – Over the Road Bus (PT-OTRB) Information Sharing & Analysis Center (ISAC). The ISAC produces and transmits daily Transit and Rail Intelligence Awareness Daily (TRIAD) reports, OTRB ISAC Daily Reports, and Daily Open Source Cyber Reports. The reports, articles, and commentaries in the TRIAD and OTRB Daily Reports are focused 24/7 on immediately analyzing and reporting information with respect to Security and Terrorism, Suspicious Activities and Incidents, Counter-Terrorism, Security Awareness, Continuity of Operations (COOP), and Cyber Security. APTA also develops, publishes and shares Security Recommended Practices with industry partners. TSA also established the Surface Intel-Information Sharing Cell (SISC) to develop an institutional framework to provide and manage sustained surface transportation intelligence and information sharing capabilities.

Further, upon stakeholder request and funding, stakeholders can utilize the Virtual Common Operating Platform (VCOP) that was built on the legacy Intermodal Virtual Imaging Enhancement Workshop (IVIEW) program alongside local, city, state and federal transportation operators, first responders, law enforcement officials, and security personnel to prepare for emergency situations. VCOP is a state-of-the-art interactive training response and exercise tool that utilizes a virtual 360-degree walkthrough of a transportation facility, such as an airport or subway station, allowing first responders to place themselves in the operating environment. The technology allows for real-time discussions on approach, access, and obstacles for first responders.

Forums for sharing information between stakeholders and TSA are firmly established, including the Aviation Security Advisory Committee (ASAC) and the recently formed Surface Transportation Security Advisory Committee (STSAC). The ASAC was established in 1989 after the terrorist attack on Pan Am Flight 103. This Committee provides advice to the TSA Administrator on aviation matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security. The ASAC is also comprised of a diverse group of individuals representing private sector organizations affected by aviation security requirements. TSA continues to use coordinating councils and industry conference calls in addition to the STSAC to maintain robust information sharing mechanisms.

The STSAC was formed in 2019 and also plays an instrumental role in enhancing situational awareness and promoting informational discussions in the surface mode. The STSAC is comprised of a broad and diverse group of persons representing each of the surface modes of transportation, as well as relevant federal government agencies. Like the ASAC, the STSAC will advise the TSA Administrator on key surface transportation security matters, including the development, refinement, and implementation of policies, programs, initiatives, rulemakings, and security directives pertaining to surface transportation security.

Recommendation 4: Expand Threat Awareness Education

Threat awareness education that promotes the exchange of relevant information is an effective method of preventing incidents. Reporting of suspicious activity is strengthened through situational awareness campaigns like “If You See Something Say Something” and local security awareness and reporting programs that preceded community outreach programs.

Aviation employs TSA's "*This is My Airport*" training program, which encourage members of the community to take a more proactive role in security. Because some aspects of security training may be considered sensitive, each organization should determine the level of training necessary to raise awareness based on individual areas of responsibility. One major airline rolled out a training program for their employees and contractors, focused on defining "See Something." This will further threat awareness by educating thousands of aviation workers on what is suspicious activity and what should be reported.

First Observer Plus™ is a surface transportation security awareness training program that focuses on delivery of a simple message to transportation professionals across all surface transportation sectors to "Observe, Assess and Report" suspicious activities. This message can be delivered in a facilitated group or classroom setting, or by accessing the appropriate training module from a library of online video lessons that introduce the viewer to an understanding of what may constitute a terrorist threat within their transportation work environment. The training program explores the justifications and motives offered by terrorists, identifies various stages and processes most often employed in the conduct of a terrorist act, and teaches the participant to recognize and report potential indicators. Participants are instructed not to intervene or engage suspicious persons or items but to provide the information to local law enforcement and to TSA.TSA also conducts voluntary assessments in Surface such as the Baseline Assessment for Security Enhancement (BASE). This assessment incorporates seventeen security and emergency management action items to assess the management of an agency's security program. The action items are considered foundational for a robust security risk reduction program.

Extending elements of these campaigns to public area employees—such as vendors at airports, railroads, subways, and transportation facilities; car rental vendors; local hotels; cab and limousine companies; Transportation Network Companies (TNC) such as Uber and Lyft; cleaning companies; gas station attendants; cargo operators; and general aviation members—increases threat awareness and education. It is important to educate individuals working in the public area of risks associated with threats and provide them with the tools and understanding of why it is imperative to protect critical information and identify suspicious activity. Incorporating security awareness training material—including operational security, recognizing suspicious activity, and reporting methods—into existing campaigns can further grow their exposure and success.

Recommendation 5: Develop Joint Risk Frameworks & Enhance Joint Vulnerability Assessments

Agencies should conduct joint vulnerability assessments and develop joint risk frameworks to highlight locations that are at a potential higher risk. While frameworks can be developed at the national level, they should be expanded locally. To support this effort, TSA issues the Cities and Airport Threat Assessment (CATA) to ensure both public entities and private operators have domain awareness on potential threats to estimate the attractiveness of an airport to known terrorist actors in order to rank from highest to lowest concern at a given point in time. Further, Regional Transit Security Working Groups have been formed in many major metropolitan cities to develop transportation specific strategies and frameworks to prioritize funding to remediate

risk.

TSA also integrates stakeholder feedback into the Transportation Sector Security Risk Assessment (TSSRA). TSSRA is a strategic risk assessment and learning tool for strategic risk analytics. TSSRA assesses the risk of real-world and hypothetical attack scenarios to transportation. This assessment also addresses transportation concerns and provides threat, vulnerability, consequence, and risk data for those concerns, while identifying emerging threats and vulnerabilities. TSSRA contains scenarios across six modes of transportation: International Aviation, Domestic Aviation, Mass Transit & Passenger Rail, Freight Rail, Pipeline, and Highway & Motor Carrier. The information in TSSRA enhances domain awareness, supports the identification of trends and vulnerabilities, and helps drive security priorities and requirements.

Maximize Prevention

Extremist propaganda, such as in al-Qa'ida in the Arabian Peninsula's English-language magazine Inspire, and the Islamic State of Iraq and the Levant's magazine Dabiq, explicitly calls for attacks on civilian targets. The 2016 attacks at Brussels International Airport and metro station, Istanbul's Ataturk Airport, the 2017 attack at Ft. Lauderdale International Airport, and the 2017 Manhattan, New York improvised low-tech explosive device attack on a mass transit system underscore the vulnerability of locations outside the secure areas of airports and the need to implement strategies to prevent and respond to such attacks across all public space areas in all modes of transportation.

A review of stakeholder resources—personnel, process, and technology—offers several opportunities to better align and strengthen resources to respond to various threats and improve day-to-day operations. Aligning resources across agencies and stakeholders provides for stronger attack prevention; more consistent intelligence, information sharing, and communication; fortified infrastructure; and more responsive operations. These are excellent demonstrations of aligning resources across various domains.

In addition, with the significant rise in Unmanned Aircraft Systems (UAS), developing plans to counter-UAS incidents in transportation domains is critical. The U.S. Government is working with industry on strategies to counter these threats. TSA is developing a UAS Roadmap to articulate TSA's vision over the next five years for its UAS responsibilities, integration of UAS into TSA's mission space, and accurately capture priorities, goals, and objectives associated with improving agency expertise and capacity. The scope of the roadmap is broader than just countering-UAS and the agency plans to engage with and seek feedback from the FAA before finalizing the document.

The National Risk Management Center (NRMC) is the CISA planning, analysis, and collaboration center working to identify and address the most significant risks to the Nation's critical infrastructure. Through the NRMC's collaborative efforts with the private sector, government agencies, and other key stakeholders, the CISA works to identify, analyze, prioritize, and manage high-consequence threats to critical infrastructure through a crosscutting risk management paradigm. (National Risk Management Fact Sheet)

Recommendation 6: Establish Unified Operations Centers

Some stakeholders have established Unified Operations Centers**,** either physical or virtual, to provide a collaborative shared space for all transportation stakeholders to enhance communications and situational awareness, response times during security incidents, and in general, promote unity of mission. Many transportation entities currently have their own independent Operations Centers. They can provide decision makers the ability to make and execute system-wide decisions swiftly and more adeptly.

Unified Operations Centers composed of system owners and operators, local law enforcement, U.S. Customs and Border Protection (CBP), TSA, and other stakeholders can help coordinate interagency responses for day-to-day operations, and most importantly, facilitate expeditious and coordinated responses to emergency situations. Adopting a unified command approach during an incident is essential in ensuring timely sharing of critical information and unity of effort when responding to an emergency.

While some large airports have established Airport Operations Centers (AOCs) and others have expressed interest, full-time AOCs (which may necessitate significant increased staffing, significant infrastructure modifications and capital investments) may not be effective at all airports, particularly smaller ones.

The FAA Domestic Events Network (DEN), which provides a vital tool in aviation security coordination and communications, is an example of the effectiveness of virtual coordination centers. The DEN provides a twenty-four hour real-time communications capability for numerous agency and private sector partners. The DEN allows key stakeholders a forum to communicate information ensuring that responses reflect the most appropriate risk-based decisions.

TSA will continue to work with stakeholders to support the further establishment of virtual and physical Unified Operations Centers, including providing a framework of guidance, best practices and lessons learned.

Recommendation 7: Effectively Integrate Innovative Detection Technologies

Enhancing preparedness by leveraging research and development to find resources/equipment to detect potential attacks is an essential step towards competing with emerging/evolving threats. The DHS Science and Technology Directorate is developing a layered and integrated capability to detect potential threat items at the speed of the traveling public. *See* link below for Fact Sheet:

https://www.dhs.gov/sites/default/files/publications/stetd_2019-fact-sheet_29apr19-508.pdf

The FAA Reauthorization Act of 2018 included a new provision extending Airport Improvement Program (AIP) eligibility to closed-circuit TV systems (CCTV). These systems play a key role in day-to-day airport surveillance and monitoring operations.

The TSA Intermodal Division (IMD) is committed to assisting stakeholders by providing

security technology recommendations and solutions by evaluating advanced technologies and developing requirements for new security capabilities for airport perimeter, airport exit lanes, lobbies and public spaces, mass transit and passenger rail, other surface transportation means, critical infrastructure, and public area venues. Because infrastructure protection of airport perimeter and public areas is highly analogous to the similar areas within transportation modes, similar technologies can be applied to multiple venues.

The Surface Security Technology (SST) Section within IMD develops technical requirements and evaluates security solutions for surface transportation modes (including mass transit & passenger rail, freight rail, pipeline, highway motor carrier, and maritime) critical infrastructure and public areas. Through close collaboration with end-users, technical experts, intergovernmental partners, and industry, IMD leverages robust processes in capability gap identification, scouting, testing, assessment, and communication to integrate technology solutions into intermodal security operations.

SST-assessed technologies undergo robust laboratory evaluations and field testing in live test bed environments to validate vendor claims. SST also provides information on TSA evaluated security technologies to the intermodal transportation community through the Surface Transportation Sensor Catalog, live technology demonstrations, industry outreach, and at request to assist stakeholders with procurement decisions, grant applications, and/or the development of Concept of Operations.

The Surface Transportation Sensor Catalog is organized by type of technology and consists of over 50 concise "For Official Use Only" (FOUO)-level summaries and corresponding test results on current commercial off the shelf technologies and legacy systems. Example capabilities include Intrusion Detection, Trace Detection, People Screening, and Intelligent Video & Video Monitoring Systems. For more information, please contact IMD at TSAIMDINFO@tsa.dhs.gov.

Recommendation 8: Vetting for Public Area Workers

Employees, tenants, contractors and other authorized personnel working in the public area of an airport or other transportation venue play an important role in the security and safety of the people and operations. Accordingly, airport and surface entities should consider conducting background checks and threat assessments to vet employees working in the public area. Some transportation entities are already implementing this approach by issuing public area ID cards and are implementing vetting programs. These IDs, issued by transportation entities to public area employees, allow better awareness of who is working within their transportation domains.

The decision to issue these IDs should be based on the unique security considerations of each area and may trigger vetting of these individuals by TSA or other qualified parties. This combination of capabilities—each transportation entity's knowledge of which public area personnel should be vetted based on the characteristics of that domain, provides an effective mitigation strategy with real-time situational awareness, knowledge of the public area workforce, and a greater capability to identify employees with intent to harm. In addition, entities implementing vetting requirements need to provide adequate redress procedures and comply with 49 CFR 1570.13 (False statements regarding security background checks by public transportation agency or railroad carrier), as applicable.

Specifically related to surface transportation, APTA and industry published a recommended practice guide for transit agencies to select security background investigation methodologies and to establish policies and procedures for conducting background investigations. This document can be found at APTA's website www.apta.com.

Recommendation 9: Workforce Employee Training

In order to effectively counter threats, a two-pronged approach of initial and recurrent training coupled with reinforced strategic communications should be part of every transportation entity's investment in their workforce. Both government and private sector entities should provide training commensurate with their security responsibilities and the scope of the individual's responsibilities. However, varied and inconsistent forms of communication are used to reach different sectors of the workforce, but a shared lexicon with consistent and strong communications could strengthen training and response. By providing a common vocabulary and understanding of how to solve problems through education and training, agencies can work together more seamlessly.

Training should occur across multiple government and transportation entities—including public area vendors and employees—at all levels throughout the organization. A key aspect of that training should include education for employees to enhance their ability to recognize and communicate potential threats to law enforcement. Learning should be applied through training exercises that incorporate every entity that plays a role during an incident. Exercises should make participants familiar with the layout of a facility (for example, public areas of an airport or multi-modal transportation station) so that in the event of an incident, first responders and others will be oriented to their surroundings.

Recommended realistic training scenarios should include at a minimum, emergency planning, active attacker ("Run, Hide, Fight"), vehicle ramming, disaster response, insider threat, and the use of trauma emergency casualty care kits. Training also should incorporate cultural and religious awareness aspects to better equip and empower the workforce. Such training, used with CBP's Tactical Terrorism Response Teams and other law enforcement organizations, helps the workforce understand certain communities that are specifically targeted for radicalization to violence.

CISA's Infrastructure Security Division offers a wide array of free training programs to government and private sector partners. These web-based independent study courses, instructor-led courses, and associated training materials provide government officials and critical infrastructure owners and operators with the knowledge and skills needed to implement critical infrastructure security and resilience activities.

Recommendation 10: Develop, Conduct, and Practice Exercises & Response Drills

Exercise and response drills provide law enforcement and other first responders the opportunity to identify obstacles to incident response. This practice should expand to include all community members—every individual or organization that would respond to an actual threat.

All must work as one to resolve realistic attack scenarios in order to prepare for real world

events. These collaborative engagements help develop strategies for incident management and identify areas requiring additional partnerships or resources.

Most aviation entities are required to conduct tabletop or other security-related types of exercises. These exercises are conducted with the participation of aircraft operators and official airport tenant first responders as well as TSA and other law enforcement agencies. The frequency of these exercises varies on the size of the facility and are structured to identify areas of responsibility. Further, airports have implemented better methods to share information including regular security meetings and other arrangements to include suspicious activity detection and other security activities on or around airport property. "If You See Something, Say Something"™ is a national campaign established to raise public awareness of suspicious indicators and report suspicious activity and as mentioned above, other campaigns related to active shooter exercises include drills such as "Run, Hide, Fight."

Training, drills, exercises, and strategic planning are also important to surface transportations systems. These systems are generally open environments, where very little is known about the travelers. Security challenges unique to these open-by-nature transportation systems can be mitigated by collaboration between surface transportation industry and security stakeholders.

TSA's Intermodal Security Training and Exercise Program (I-STEP) provides exercise, training, and security planning tools and services to the transportation community. The program focuses on the security nexus of the intermodal transportation environment, serving mass transit and passenger rail, freight rail, pipeline, port and intermodal, highway and motor carrier, and aviation modes. Drills and exercises are effective tools to prevent, protect, mitigate, respond, and recover from real-world attacks.

Working in partnership with the transportation modes, I-STEP enables security partners to:

1. Enhance security capabilities – strengthen plans, policies, and procedures; clarify roles and responsibilities; validate planning needs; and strengthen grant proposals.
2. Build partnerships – develop relationships with regional transit players and other stakeholders.
3. Gain insights in transportation security – network with peers to gain a deeper understanding of security lessons learned and best practices.

For example, in October 2018, I-STEP convened a Southern California Regional Intermodal Security Exercise (RISE) one-day workshop and facilitated discussions at the U.S. Armed Forces Reserve Center in Bell Gardens, CA. The exercise included representatives from all five surface transportation modes (Highway and Motor Carrier, Mass Transit and Passenger Rail, Pipeline, Freight Rail, and Maritime) as well as representation from five CA counties. Participants identified the most relevant regional security challenges facing surface transportation systems and determined actions necessary to increase their ability to deter, detect, and interdict against evolving attack types. Through this exercise, TSA and the stakeholders successfully:

- Introduced Southern CA stakeholders to federal, regional, state, local, and

private sector counterterrorism resources, capabilities, technologies, personnel, and initiatives;
- Informed best practices and improve information sharing; and
- Evaluated prevention- and protection-related capabilities, plans, resources, and coordination.

The I-STEP RISE leveraged the experience of 112 federal, local government and multi-modal industry partners.to significantly increase/enhance connectivity, partnerships, and awareness of capabilities and resources.

Infrastructure and Public Protection

Recommendation 11: Invest in Innovative Construction Designs

As transportation venue infrastructure seeks to keep pace with trends in the travel industry, technological changes, and security requirements, it is imperative that construction designs are reviewed. Designs should incorporate more than just an aesthetic perspective; they should facilitate effective security while remaining sensitive to stakeholder needs. Future airport and surface transportation station and facility designs need to balance between depicting the feel of an open and welcoming environment and increasing the overall security measures of the facility. To achieve that balance, transportation venue-designers need to build in security measures within their designs, not bolt on after the design is created, whether it is for an airport or new public transportation/bus station.

TSA has several design guidelines available for airports that focus on construction development as well as checkpoint screening designs. The Checkpoint Requirements and Planning Guide (CRPG) is intended to help airports to improve their current checkpoints and plan for the future based on both current screening solutions and anticipated future innovations. The document provides key information on equipment, design requirements, and other key details to support both the development of flexible checkpoint spaces today and the ability to plan and adapt to future checkpoint needs. TSA developed the CRPG in close consultation with industry throughout the process. TSA held a workshop in August 2018 to capture direct feedback from stakeholders and industry. The design principles and methods outlined in the CRPG incorporate key experience from industry stakeholders. TSA is grateful for the feedback and collaboration from industry stakeholders throughout this process.

https://www.fbo.gov/index?s=opportunity&mode=form&id=6d618178938d8fa31d64fc097587bcbb&tab=core&_cview=1

The recommended Security Guidelines for Airport Planning, Design and Construction represents the fifth iteration of guidance for the airport security planning and design community, first issued by the FAA in 1996 and 2001, continued by the TSA in 2006 and 2011, and now provided by National Safe Skies Alliance. All have had extensive participation in and contributions of content by federal agencies, industry trade associations, and individual architects, engineers, security consultants, and other subject matter experts. The periodic updates have been driven largely by constant changes in both physical and digital technologies, as well as national and

international standards, policies, and operational requirements that reflect the changing aviation threat environment.

The Guidelines are not government regulations and requirements; they are a compendium of real-world experience and best practices developed by outstanding professionals in the field, providing recommendations for airport security–specific planning and design concepts that are scalable to airports of any size and complexity. This document can be found on the Safe Skies website.

https://www.sskies.org/paras/reports

The Crime Prevention Through Environmental Design (CPTED) for Transit Facilities Recommended Practice (RP) is a good example of a surface transportation resource that provides guidance on construction designs. The RP was developed as a result of a collaborative effort between TSA, APTA, and industry partners.

https://www.apta.com/wp-content/uploads/Standards_Documents/APTA-SS-SIS-RP-007-10.pdf

During the onset of designing a transportation facility, designers should convene and interview all appropriate stakeholders to get a better understand of vulnerabilities across the enterprise. This will allow designers to think holistically at all aspects of what the needs are. There are locations within a venue where security—like cameras, guards, and metal detectors— should be visible, in lobbies and other open area locations security may be more discreet.

The initial conversations between stakeholders should be the start of ongoing communication and collaboration. Because threats evolve and nefarious actors are extremely agile, corresponding technology and designs to thwart those threats must also evolve and be agile. To achieve this, security goals need to be discussed and shared. Designers, working with security stakeholders, should think ten to fifteen years down the road. Putting the right infrastructure in place now saves time, energy, and financial resources in the future.

Identifying the people, process, and technology elements of an effective security system and establishing a framework for incorporating these areas into facilities should be a high priority when designing for security. Additionally, the development of flexible guidance—identifying security risks and corresponding mitigation plans—should be incorporated into design efforts for both new construction and renovation of pre-existing facilities.

In January 2017, Public Area Security Summit members convened in Chicago to observe real world examples of renovation and new construction projects at Chicago Midway International Airport and O'Hare International Airport. Members met with industry subject matter experts to identify areas of need and security focus. The Chicago airports serve as "field labs" to discuss and review best practices for Public Area Security design and infrastructure changes.

Recommendation 12: Coordinate Response Planning

The most basic form of deterring, detecting, and defeating potential attacks is through the

performance of daily security operations. The presence of law enforcement and security personnel provides a visible deterrent against adversaries. Doing so may prevent attacks, or in the event of an attack, allow first responders to respond more adeptly. Furthermore, given the potential for fixed-post law enforcement officers to be the first target of an attack, individual airports and transportation venues should strategize on the appropriate deployment of law enforcement officers and/or contracted security.

Visible deterrence is a critical element of the Law Enforcement Reimbursement Program (LEO RP). The LEO RP provides partial reimbursement to airport operators to provide on-site, visible LEO presence through flexible, fixed, or a combination of the two (hybrid) support of TSA passenger screening activities at checkpoints to detect, deter, and mitigate criminal threats and counter terrorism activities. State and local LE agencies play a critical role in security at airports. They are the primary responders to any incident within the airport perimeter, including TSA checkpoints.

When performing routine operations in the public area, law enforcement personnel should deploy a variety of tactics, including the use of both fixed posts and random patrol areas, as well as canines. Depending on the venue's needs (e.g., high-visibility presence to deter attackers, surveillance operations), law enforcement may elect to conduct patrol operations in plain clothes or uniform. When feasible, law enforcement should deploy appropriately trained canine teams in a manner that increases visibility, minimizes response times to incidents, and deters individuals from engaging in criminal activity. Canine handlers should be trained on procedures for resolving canine alerts and capable of balancing law enforcement's responsibility to take action with the civil rights of passengers.

When responding to an incident, law enforcement should utilize non-traditional locations (for example, shuttles) as shelters during evacuations. However, first responders should consider the conditions of such locations (such as weather and/or capacity) and their vulnerability to coordinated ambushes. Law enforcement response plans must be flexible to deploy specialized tactics in response to varied situations. To maintain these capabilities, law enforcement must have adequate access to resources, including manpower and funding for equipment and training.

Conclusion

The partnerships established by the Public Area Security Summits and 2019 working group do not cease with these Best Practices. The working group is committed to engaging and collaborating with, and providing options to, partners, which includes identifying organizations or individuals who have not traditionally been incorporated into either Aviation or Surface transportation security plans.

Meetings and calls will continue periodically, in order to affirm partnerships and continue reviewing solutions to improve public area security. The group will continue to incorporate additional stakeholders as necessary to ensure additional aspects of public area security are represented.