United States Government Accountability Office

Report to Congressional Requesters

AVIATION SECURITY

TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals

Accessible Version

February 2020

GAO-20-275

GAO Highlights

Highlights of GAO-20-275, a report to congressional requesters

February 2020

AVIATION SECURITY

TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals

Why GAO Did This Study

Aviation workers using their access privileges to exploit vulnerabilities and potentially cause harm at the nation's airports is known as an "insider threat." TSA, airport operators, and air carriers share the responsibility to mitigate all insider threats at airports. In October 2019, TSA estimated there are about 1.8 million aviation workers at the nation's airports.

GAO was asked to review TSA's and aviation stakeholders' efforts to mitigate insider threats at airports. This report (1) discusses the efforts that TSA, airport operators, and air carriers have taken to help mitigate insider threats at airports and (2) evaluates the extent to which TSA's Insider Threat Program is guided by a strategic plan and has performance goals.

GAO reviewed TSA guidance; analyzed TSA data from a questionnaire sent to a representative sample of airport operators; and obtained information from TSA officials, officials from selected larger U.S.-based air carriers, and a nongeneralizable sample of seven airport operators, selected, in part, based on the number of aircraft take-offs and landings.

What GAO Recommends

GAO recommends that TSA develop and implement a strategic plan that has strategic goals and objectives, and develop performance goals to assess progress achieving objectives in the strategic plan. TSA agreed with GAO's recommendations.

View GAO-20-275. For more information, contact Triana McNeil at (202) 512-8777 or McNeilT@gao.gov.

What GAO Found

The Transportation Security Administration (TSA), airport operators, and air carriers mitigate insider threats through a variety of efforts. TSA's Insider Threat Program comprises multiple TSA offices with ongoing insider threat mitigation activities, including long-standing requirements addressing access controls and background checks, and compliance inspections. TSA also initiated activities more recently, such as implementing TSA-led, randomized worker screenings in 2018. Airport and air carrier officials implement security measures in accordance with TSA-approved programs and may implement additional measures to further mitigate threats. For example, many airport operators reported using sophisticated access control technologies (e.g. fingerprint readers). Additionally, some air carriers reported conducting more rigorous background checks prior to issuing identification credentials to employees.

Examples of Methods to Mitigate Insider Threats at U.S. Airports

Source: GAO presentation of Transportation Security Administration information. | GAO-20-275

TSA's Insider Threat Program is not guided by a strategic plan with strategic goals and objectives nor does it have performance goals.

- TSA does not have an updated strategic plan that reflects the Program's current status. TSA officials said that the plan was not updated due to turnover of key senior leadership. As of January 2020, TSA officials said they were developing a roadmap that could serve as a new strategic plan for the Program. However, officials had not finalized the contents and were uncertain when it would be completed and implemented. Developing and implementing a strategic plan will help guide TSA's ongoing efforts and coordinate TSA's agency-wide approach.
- TSA has not defined performance goals with targets and timeframes to assess progress achieving the Program's mission. Without a strategic plan and performance goals, it is difficult for TSA to determine if its approach is working and progress is being made toward deterring, detecting, and mitigating insider threats to the aviation sector.

Contents

Tables

Figures

Abbreviations

ASAC	Aviation Security Advisory Committee
ATLAS	Advanced Threat Local Allocation Strategy
SIDA	Security Identification Display Area
TSA	Transportation Security Administration

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

February 10, 2020

The Honorable Mike Rogers
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Debbie Lesko
Ranking Member
Subcommittee on Transportation and Maritime Security
Committee on Homeland Security
House of Representatives

The Honorable John Katko
House of Representatives

The Honorable Michael McCaul
House of Representatives

In 2019, the Transportation Security Administration (TSA) estimated that there were more than 1.8 million aviation workers with unescorted access to security-restricted areas of the nation's airports.[1] The insider threat—in which an aviation worker uses their access privileges and knowledge of security procedures to exploit vulnerabilities of the civil aviation system and potentially cause harm—is one of TSA's most pressing concerns.[2] TSA has consistently identified the vulnerability of the aviation system to

[1]For the purposes of this report, "security-restricted area" is a general term that encompasses areas of a commercial airport, identified in an airport operator's TSA-approved security program, for which access is controlled and limited and includes areas accessible to passengers who have passed through a security checkpoint.

[2]For the purposes of this report, an "aviation worker" is an employee, contractor, or representative of an airport operator, U.S. or foreign-flagged (i.e., domestic or foreign) air carrier (including flight and cabin crew), vendor, concessionaire, tenant, government agency (including TSA), entity in the air cargo supply chain, or other entity who may at any time work or conduct operations at an airport or areas adjacent to or connected with an airport (including an entity's supply chains) subject to regulation by TSA. In addition, for the purposes of this report, we use the term "air carriers" to include both aircraft operators (i.e., U.S.-based air carriers) operating in accordance with 49 C.F.R. part 1544, and foreign air carriers operating in accordance with 49 C.F.R. part 1546.

the insider threat among its highest enterprise-level risks.[3] Recent incidents where aviation workers stole or damaged an aircraft or smuggled illegal drugs, firearms, and cash have highlighted this threat. For example, in July 2019, an aircraft mechanic was charged with willfully attempting to damage an aircraft. Additionally, in August 2018, a ground services agent commandeered a small aircraft, which subsequently crashed. Insider threats may arise from a malicious intent to cause harm, or may arise from workers assuming a negligent or ignorant approach to security procedures and potential risks. In an effort to help mitigate insider threats at commercial airports, TSA established its Insider Threat Program in 2013.[4]

You asked us to review what TSA and its aviation security stakeholders are doing to mitigate risks of the insider threat at the nation's commercial airports. This report (1) discusses the efforts of TSA, airport operators, and air carriers to help mitigate insider threats at commercial airports and (2) evaluates the extent to which TSA's Insider Threat Program is guided by a strategic plan that includes strategic goals and objectives, and has established performance goals.

To determine what efforts TSA has implemented to mitigate insider threats at commercial airports, we reviewed TSA's programmatic guidance on the Insider Threat Program, including the charter that established the program. We also reviewed relevant policies, procedures, and notices, as well as applicable statutes, regulations, and security directives. We interviewed TSA officials responsible for the individual programs that make up TSA's Insider Threat Program, including officials from Law Enforcement/Federal Air Marshal Service; Security Operations; Policy, Plans, and Engagement; and Intelligence and Analysis to obtain information on the efforts the agency has implemented to enhance the program. We also interviewed TSA federal security directors or their

[3]Transportation Security Administration, *TSA Enterprise Risk Register* (May 2019). TSA considers its ability to respond to emerging and evolving threats as its highest enterprise-level risk.

[4]For the purposes of this report, a "commercial airport" is an airport in the United States operating under a TSA-approved security program in accordance with 49 C.F.R. part 1542 and that, in general, regularly serves air carriers with scheduled passenger operations (also referred to as "TSA-regulated airports"). Most commercial airports discussed in this report, which, in general, are those regularly serving air carriers with scheduled passenger operations in accordance with 49 C.F.R. parts 1544 and 1546, operate under "complete" security programs, which contain the most comprehensive security measures. See 49 C.F.R. § 1542.103(a).

representatives at a non-generalizable sample of seven commercial airports to discuss and observe how TSA policies and procedures related to mitigating insider threats are implemented at airports.[5] Additionally, they provided insight regarding how officials at TSA compliance hubs (field offices) coordinate with airport operators and air carriers to mitigate threats. We selected the sample of airports to include (1) airports that had experienced an insider threat security incident since the beginning of fiscal year 2017, (2) airports from each TSA airport category, and (3) a geographic distribution of airports across the country.[6] We also incorporated input from stakeholders into our airport selection. Although results from these interviews and site visits are not representative, they provide information on the views of field-based TSA officials and illustrative examples of how TSA policies are implemented at commercial airports.

To determine what efforts airport operators have implemented to mitigate insider threats, we analyzed TSA data collected from a representative sample of airport operators. TSA administered its questionnaire to all category X and category I airports and a stratified random sample of category II, III, and IV airports as part of a TSA information circular.[7] Respondents replied to the questionnaire by submitting answers into an electronic system. TSA then shared the exported database with GAO for analysis. The questionnaire, which TSA had previously issued to airport operators in 2016, asked compliance hubs (field offices) to provide a snapshot-in-time of current airport operator and air carrier policies and procedures related to the use of intelligence, aviation worker training courses, control of credentials that allow access to security-restricted areas, control of access to secured and sterile areas of the airport, and aviation worker screening, among other topics. To assess the reliability of these data, we reviewed related documentation from TSA and relevant

[5]Among other things, federal security directors are the ranking TSA authorities responsible for leading and coordinating TSA security activities at the nation's commercial airports.

[6]TSA classifies the nation's approximately 430 commercial airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, category X airports have the highest number of passenger enplanements and category IV airports have the fewest.

[7]See TSA Information Circular 15-01E, August 30, 2018. TSA may issue an information circular to notify airport operators and other regulated entities of security concerns. See, e.g., 49 C.F.R. §§ 1542.303(a) (airport operators), 1544.305(a) (aircraft operators). TSA also requested information about the air carriers with exclusive area agreements at the sampled airports; however, we did not analyze the data from these entities as part of our review.

program offices regarding the systems used to collect and store the data; interviewed TSA officials from relevant program offices regarding the reliability of the data received; electronically tested the data for missing data and obvious errors; and corroborated the contents of entries with testimonial evidence collected from airport operator officials for a sample of airports. We found these data to be sufficiently reliable for reporting descriptive statistics about the efforts of airport operators to mitigate insider threats. During our site visits to seven airports, we observed airport operations and access control technologies in use and discussed security activities and other measures to mitigate insider threats with airport officials. We also discussed how the airport operator collaborated with TSA and other aviation stakeholders to carry out these mitigation measures. Further, we interviewed officials from two airport industry associations with specialized knowledge and experience with airport security and insider threats to obtain information on efforts underway at commercial airports to help mitigate insider threats.

To determine what efforts air carriers have implemented to mitigate insider threats, we interviewed officials from a non-generalizable sample of six of the largest U.S.-based air carriers about their efforts to mitigate insider threats.[8] Information obtained through these interviews is not generalizable to all air carriers, but provides us with illustrative information on air carriers' use of access control technologies, aviation worker training and assistance programs, and aviation worker screening, among other topics. Further, we interviewed officials from one air carrier industry association to obtain information on the industry's practices and measures to mitigate insider threats.

To determine the extent to which TSA is guided by a strategic plan with strategic goals and objectives, and has performance goals that could be used to assess progress toward achieving strategic objectives, we reviewed programmatic guidance for TSA's Insider Threat Program, including the 2014-2016 TSA Insider Threat Action Plan (Action Plan) and the August 2019 Insider Threat Response Plan.[9] We also reviewed TSA's *Administrator's Intent* to identify the ongoing initiatives related to the

[8]The U.S. Department of Transportation groups U.S.-based air carriers according to the operating revenue boundaries contained in 14 C.F.R. § 241(4). As of January 1, 2020, 18 air carriers are included in Carrier Group III, which includes U.S.-based air carriers who reported operating revenue greater than $1 billion for a twelve-month period.

[9]Transportation Security Administration, *Insider Threat: FY2014-2016 Action Plan* (April 2014).

Insider Threat Program,[10] as well as reports issued by the Aviation Security Advisory Committee (ASAC) that, among other things, recommend actions TSA should take to enhance its ability to carry out its mission to deter, detect, and mitigate the insider threat.[11] We interviewed TSA officials and obtained information from TSA's Insider Threat Executive Steering Committee on the extent to which the agency has developed a strategic plan and performance goals. We compared the information collected through our review of documentation and interviews with agency officials with standards and recommendations for insider threat programs made by the National Insider Threat Task Force as well as *Standards for Internal Control in the Federal Government*.[12] We also considered the GPRA Modernization Act of 2010 requirements as described in guidance by the Office of Management and Budget.[13]

We conducted this performance audit from January 2019 to February 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.

[10]Transportation Security Administration, *Administrator's Intent* (June 1, 2018).

[11]Established in 1989 in the wake of a terrorist attack on Pan Am flight 103—commonly referred to as the "Lockerbie bombing"—ASAC provides advice to the TSA Administrator on aviation security matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives. Committee members represent stakeholder groups affected by aviation security requirements. The Aviation Security Stakeholder Participation Act of 2014, enacted in December 2014, established the ASAC in statute. See 49 U.S.C. § 44946.

[12]National Insider Threat Task Force, *Insider Threat Program Maturity Framework* (Washington, D.C.: November 1, 2018); GAO, *Standards for Internal Control in the Federal Government*, GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

[13]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, OMB Circular A-11 (revised July 2016).

Background

Airport Security Roles and Responsibilities

As the federal agency with primary responsibility for civil aviation security within the United States, TSA promulgates security requirements, primarily through regulations but also through security directives and other mechanisms, and conducts inspections to ensure that airport operators, air carriers, and other regulated entities are in compliance with these requirements.[14] Additionally, TSA oversees security operations at airports through different types of testing and vulnerability assessments to analyze and improve security, among other activities. As of December 2019, there were approximately 430 commercial airports nationwide.

Airport operators, air carriers, and other regulated entities are responsible for implementing security requirements, primarily in accordance with their TSA-approved security programs. These programs generally cover day-to-day operations, including measures that contribute to mitigating insider threats.[15] For example:

- For most commercial airports, airport operators must ensure there is an adequate law enforcement presence to support operations and prevent unauthorized access to security-restricted areas through,

[14]See Pub. L. No. 107-71, 115 Stat. 597 (2001); 49 U.S.C. § 114(d). See also, e.g., 49 C.F.R. §§ 1542.5 (airport inspections), 1544.3 (domestic air carrier inspections), and 1546.3 (foreign air carrier inspections). When TSA determines that additional security measures—beyond what are required of regulated entities to implement in existing regulations—are necessary to respond to a specific threat assessment or to a specific threat against civil aviation, TSA may issue security directives (or emergency amendments, in the case of foreign air carriers) that set forth mandatory measures. See, e.g., 49 C.F.R. §§ 1542.303(a), 1544.305(a), 1546.105(d).

[15]See, generally, 49 C.F.R. ch. XII, subch. C. In general, TSA-approved security programs describe the policies, procedures, and systems the airport operators, air carriers, and other regulated entities implement to comply with TSA requirements. For purposes of this report, we use the term “TSA-approved” to include the security programs of foreign air carriers, but recognize that TSA regulations provide that the security programs for foreign air carriers must be deemed acceptable by TSA. See 49 C.F.R. § 1546.103.

among other measures, employee vetting, the use of personnel identification media, and implementing access control systems.[16]

- For most air carrier operations, the air carriers must implement measures to ensure the security of aircraft and facilities, such as preventing unauthorized access to aircraft; searching aircraft prior to boarding passengers; randomly searching service personnel, such as caterers, and their property prior to boarding the aircraft; and training employees in security procedures.

In accordance with an airport operator's security program, an air carrier may enter into an agreement with the airport operator to assume exclusive responsibility for specified security measures for all or portions of an airport's security-restricted areas, including access points.[17] This is known as an exclusive area agreement.

The security programs that airport operators and air carriers implement, in accordance with federal regulations, are generally consistent across similarly-situated airports and air carriers. For example, all airports operating under complete security programs generally implement TSA-approved security programs that address the same requirements.[18] However, the details of these programs and their implementation can differ widely based on the individual characteristics of the airport. For example, methods that airport operators use to control access into security-restricted areas vary because of differences in the design and layout of individual airports, but all access controls must meet minimum

[16]These airports, which, in general, are those regularly serving air carriers with scheduled passenger operations in accordance with 49 C.F.R. parts 1544 and 1546, operate under "complete" security programs that contain the most comprehensive security measures. See 49 C.F.R. § 1542.103(a). The remaining commercial airports generally adopt and implement "supporting" or "partial" security programs that contain fewer requirements. See 49 C.F.R. § 1542.103(b), (c). In this report, all mentions of an airport security program refer specifically to a complete security program unless otherwise indicated. According to TSA officials, airports classified by TSA as categories X, I, II, and III must operate under complete security programs, with some category IV airports operating under complete security programs as well.

[17]See 49 C.F.R. § 1542.111.

[18]It is possible, however, for security programs to vary even when subject to the same general requirements. For example, an airport operator may pursue an amendment to its security program that, if approved, may distinguish that airport's practices from those of its peer airports. See 49 C.F.R. § 1542.105. TSA may also issue security directives setting forth requirements when it determines that additional security measures are necessary to respond to a threat assessment or a specific threat against civil aviation. See 49 C.F.R. § 1542.303. Such directives, however, typically afford airport operators the opportunity to request alternative means of implementation, which if approved could likewise distinguish its practices from those of other airports subject to the particular directive.

performance standards in accordance with TSA requirements. Airport operators and air carriers may also choose to implement measures beyond what is required by TSA, but they may choose not to pursue incorporating these additional measures into their security programs, because if incorporated into their security programs, TSA could then hold the regulated entities accountable for implementing such additional measures. By not incorporating the additional measures into their security programs, airport operators and air carriers retain the flexibility to alter such measures without TSA approval.

The security measures that airport operators and air carriers implement are generally carried out within, or to prevent access to, security-restricted areas of an airport or aircraft. These areas include:

- **Secured areas.** Areas for which security measures, such as access controls, must be carried out to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles. This includes areas where domestic and foreign air carriers enplane and deplane passengers and sort and load baggage, and any adjacent areas not separated by adequate security measures.
- **Security identification display areas (SIDA).** Areas for which security measures, such as personnel identification systems, must be carried out to prevent the unauthorized presence and movement of individuals.[19]
- **Air operations areas.** Areas for which measures must be carried out to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles. This includes aircraft movement and parking areas, loading ramps, and safety areas for use by TSA-regulated aircraft, and any adjacent areas not separated by adequate security systems, measures, or procedures.[20]
- **Sterile areas.** Areas that, in general, provide passengers access to boarding aircraft and to which access is controlled through the screening of passengers and property.[21]

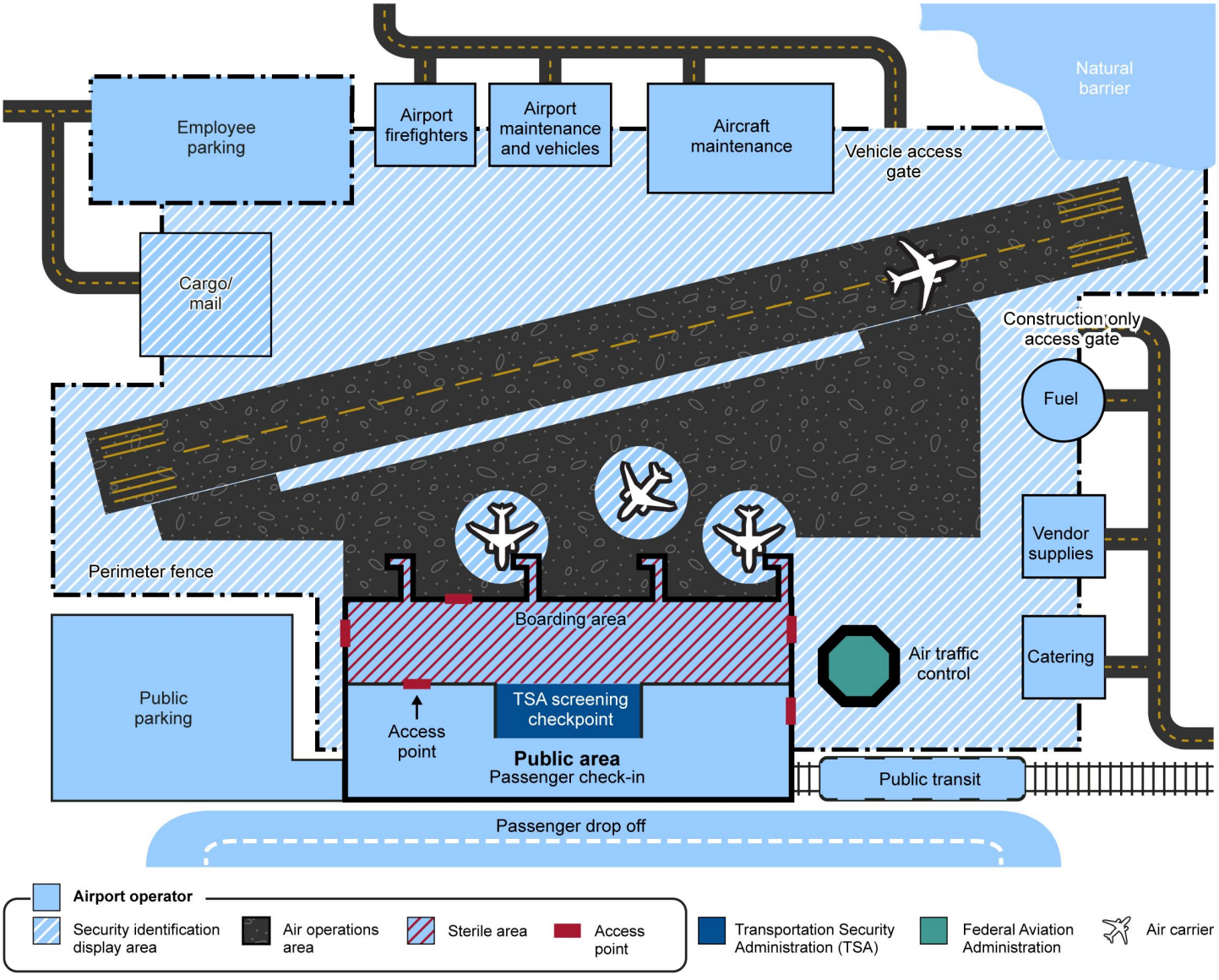
[19]SIDAs include secured areas and may include other areas of the airport.

[20]The air operations area is not a secured area but may be a SIDA.

[21]For the purposes of this report, any discussion of entry into the sterile areas of an airport or the technologies used to control access to security-restricted areas of the airport refers to entry by means other than passing through a passenger screening checkpoint, unless otherwise specified.

Figure 1 illustrates the variety of security-restricted areas of a typical larger airport, such as a category X or I airport, and aviation stakeholders' primary responsibilities for securing the area.

Figure 1: Example of Security-Restricted Areas of a Larger Transportation Security Administration (TSA)-Regulated Airport and Primary Responsibilities of Aviation Stakeholders



Source: GAO presentation of TSA information. | GAO-20-275

Note: This figure generally depicts the security-restricted areas of a TSA-regulated (i.e. commercial) airport, as designated in TSA-approved security programs and in accordance with TSA requirements. See 49 C.F.R. §§ 1542.103, 1544.103. Access points are doors (and sometimes vehicle access

gates) that are accessible to aviation workers with unescorted access to security-restricted areas. For purposes of this report, "security-restricted area" is a general term that encompasses areas of a commercial airport, identified in an airport operator's TSA-approved security program, for which access is controlled and limited and includes areas accessible to passengers who have passed through a security checkpoint. Air carrier security programs for operations at commercial airports must, in general, implement measures to prevent unauthorized access to areas under the air carrier's exclusive control and to each of its aircraft. See 49 C.F.R. § 1544.225.

TSA's Insider Threat Program and Insider Threat Incidents

TSA's Insider Threat Program, which was established in 2013, consists of offices across TSA conducting different portions of the insider threat mission, with TSA's Law Enforcement/Federal Air Marshal Service office serving as the program lead. The program's mission is to deter, detect, and mitigate insider threats to the nation's transportation sector personnel, operations, information, and critical infrastructure.[22] Other TSA offices that have key responsibilities in the Insider Threat Program include TSA's Security Operations;[23] Enrollment Services and Vetting Programs; Inspection; Intelligence and Analysis; and Policy, Plans, and Engagement, among others. To support inter-office coordination, TSA established the Insider Threat Advisory Group in 2015, which is a multi-office team of experts who review and analyze the program's activities, identify gaps, and develop mitigation strategies, among other activities. The group is co-chaired by two TSA offices—Law Enforcement/Federal Air Marshal Service and Intelligence and Analysis. TSA's Insider Threat Unit, which operates within the Law Enforcement/Federal Air Marshal Service office, serves as the focal point for all referrals of potential insider threat incidents.

According to TSA, an insider threat includes direct risks to TSA's security operations, as well as indirect risks that may compromise critical infrastructure or undermine the integrity of the aviation security system. Examples of insider threat events include compromises of airport security (e.g. using access and knowledge to smuggle contraband) and sabotage (e.g. intentionally damaging equipment meant to detect unauthorized access to security-restricted areas). TSA recognizes, however, that some insider threats may arise from complacency or ignorance rather than a

[22]Department of Homeland Security, Transportation Security Administration, *Insider Threat Program*, TSA Management Directive No. 2800.17 (July 2013).

[23]Relevant entities within Security Operations include the Compliance Directorate and the Domestic Aviation Operations Advanced Threat Local Allocation Strategy (ATLAS) program.

malicious intent to cause harm, such as when workers assume a negligent approach to policies, procedures, and potential risks.

The Insider Threat Unit receives referrals from a telephone tip line and email address; daily reports from the Transportation Security Operations Center detailing security policy violations, such as aviation workers attempting to bring prohibited items not necessary to their work duties into security-restricted areas of the airport; and internal and external intelligence reports and referrals. After a referral is made, the unit is to coordinate, disseminate, and retain all information when reviewing referrals and conducting investigations into potential insider threats. Specifically, the unit is to coordinate inquiries and investigations with the appropriate lead entities to include TSA offices; federal, state, and local law enforcement and intelligence agencies; and various airport and transit law enforcement authorities. According to one TSA official, many of these referrals do not require additional investigation because they were already appropriately mitigated at the local level. Referrals that meet the unit's criteria are accepted for further investigation—called acceptances. Criteria include, for example, whether the incident involved a prohibited item, the perpetrator has multiple violations, the perpetrator attempted to circumvent security, or the perpetrator made threatening statements.

According to Insider Threat Unit data from fiscal year 2017 through fiscal year 2019, there were an average of 138 referrals and 14 acceptances per month.[24] The majority of referrals accepted for investigation during this time period occurred at category X and I airports (63 and 25 percent, respectively). Referrals where air carrier employees and other aviation workers are the potential insider threat each account for approximately one-third of referrals accepted for investigation. Table 1 discusses examples of insider threat incidents.

[24]To assess the reliability of these data, we reviewed related documentation from TSA and relevant program offices regarding the systems used to collect and store the data; interviewed knowledgeable agency officials from TSA and relevant program offices regarding the reliability of the data received; and electronically tested for missing data and obvious errors. We found these data to be sufficiently reliable for presenting descriptive data about the frequency and selected characteristics of referrals of potential insider threat incidents.

Table 1: Examples of Insider Threat Security Incidents at Transportation Security Administration (TSA)-regulated Airports in the United States

Year(s)	Incident
2019	An aircraft mechanic at Miami International Airport used his access to aircraft to sabotage an avionics component onboard an aircraft.
2016-2018	A group of air carrier employees at Dallas-Fort Worth International Airport, including baggage handlers and others who were responsible for monitoring baggage as it was loaded onto planes, smuggled what they believed to be methamphetamine aboard flights during a two-year Federal Bureau of Investigation operation. The operation ended when agents learned that one of the employees offered to smuggle explosives onto a flight as well.
2018	A flight crew member attempted to transport packages of cocaine into the United States during a flight to John F. Kennedy International Airport from Montego Bay, Jamaica. He taped the packages to his legs, but the packages were detected by a U.S. Customs and Border Protection officer during an inspection upon arrival.
2018	An air carrier ground service agent at Seattle-Tacoma International Airport used his access to the air operations area to board an empty 76-seat turboprop plane and conduct an unauthorized takeoff. The plane subsequently crashed on a sparsely-populated island southwest of the airport.
2017	A transportation security officer (i.e. a TSA-employed screener) at Orlando International Airport was arrested for stealing cash from a traveler's carry-on bag. Closed-circuit television confirmed the theft.
2016	A flight attendant dropped a bag loaded with 70 pounds of cocaine at a Known Crewmember access point (a dedicated screening checkpoint lane for flight and cabin crew members) at Los Angeles International Airport in an attempt to avoid a random screening operation that was underway at the access point.
2016	An air carrier ramp agent at Palm Beach International Airport used his employee badge to enter the sterile area through an access point with only random screening. Once inside, he delivered a backpack containing hundreds of thousands of dollars to a passenger in a bathroom who was flying to New York.
2012-2015	A group of air carrier baggage handlers at Oakland International Airport used their employee badges to carry bags containing marijuana into the sterile area through employee access points. Once inside, they handed them off to ticketed passengers bound for other cities who had already passed through a TSA passenger screening checkpoint.
2014	An air carrier employee at Hartsfield-Jackson Atlanta International Airport used his access media to traverse an access point with only random screening outside his normal working hours. He carried guns through the access point and then handed them off to a former worker who had already passed through a TSA passenger screening checkpoint. The former worker then carried the guns in his carry-on luggage from Atlanta to New York. The two men conducted the scheme on several occasions.
2013-2014	Three screeners at San Francisco International Airport wittingly allowed carry-on bags with cocaine to pass through the X-ray machine at a passenger screening checkpoint for a fee on five occasions.
2013	An avionics technician at Wichita Mid-Continent Airport used his access media to attempt to open a vehicle security gate and drive a van loaded with what he believed were explosives onto the tarmac during a Federal Bureau of Investigation undercover investigation.

Source: GAO analysis of TSA information and news media reports. | GAO-20-275

Note: U.S. Customs and Border Protection agents inspect travel documents, and in some cases, the baggage of international travelers, including returning U.S. citizens, at U.S. international airports. See 6 U.S.C. § 211. San Francisco International Airport is one of 22 airports, as of October 2019, participating in TSA's Screening Partnership Program whereby private sector companies contract with TSA to provide screening services at TSA-regulated airports. See 49 U.S.C. § 44920.

TSA, Airport Operators, and Air Carriers Help Mitigate Insider Threats through Various Efforts

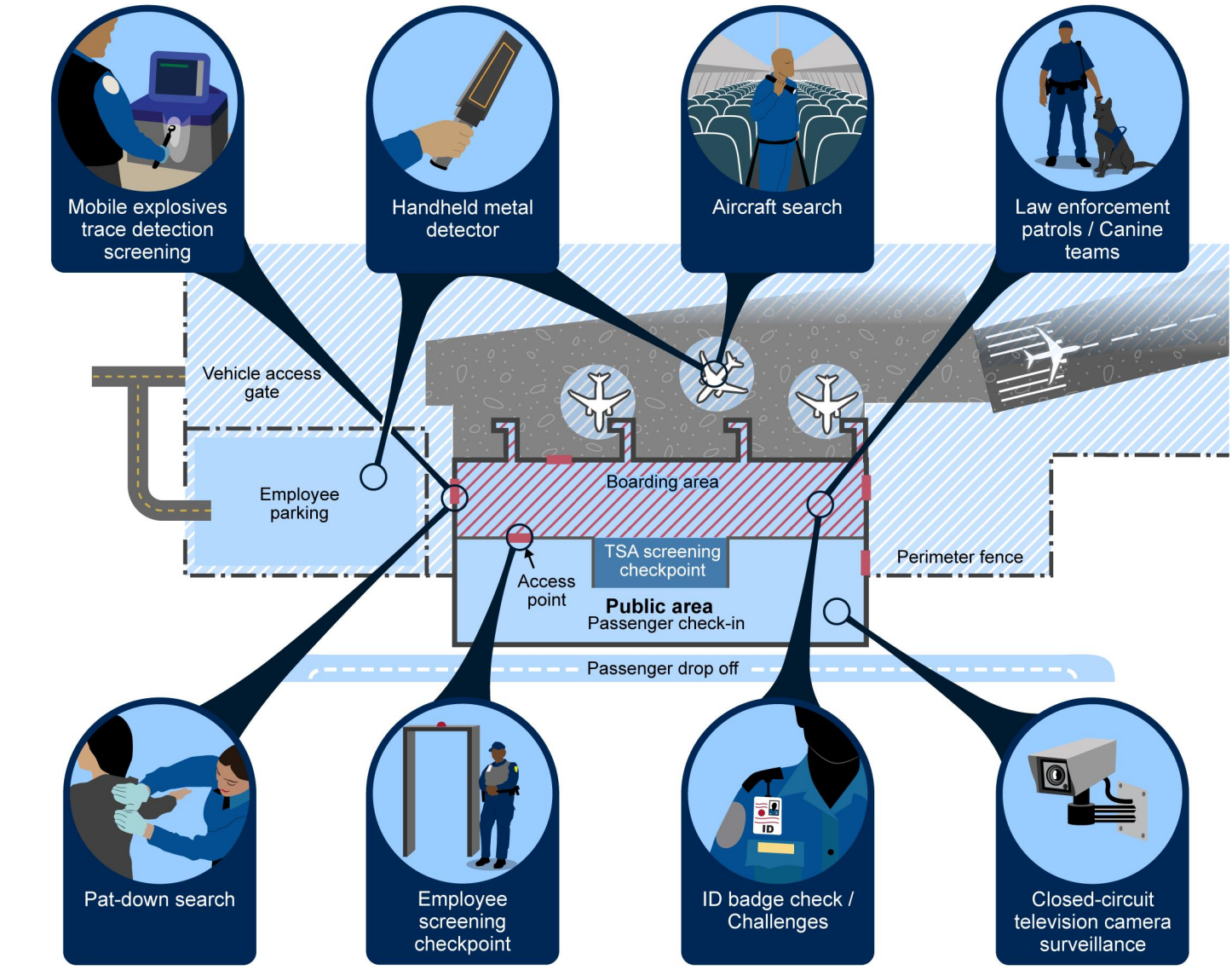
TSA has ongoing activities that help mitigate insider threats, including long-standing historical efforts and more recent efforts initiated since 2017. For example, TSA initiated operations to randomly search aviation workers at high-risk airports through pat down searches and explosives trace detection. TSA also has plans to enhance its current Insider Threat Program.

Airport operators are to implement security measures, primarily in accordance with their TSA-approved security programs, which detail the day-to-day operations of those entities and their responsibilities for controlling access to security-restricted areas, among other responsibilities. Based on our analysis of TSA's representative sample, some airport operators choose to implement security measures beyond those required by TSA. For example, some airport operators use sophisticated technologies such as fingerprint readers to control access to security-restricted areas, or offer or require training for aviation workers about topics such as insider threats.

Similarly, air carriers are to implement security measures in accordance with TSA-approved security programs. For example, air carriers are required to perform regular searches of aircraft. Some air carriers we spoke to said they also choose to implement additional measures not required by TSA to enhance their security posture, such as conducting full employee screening at dedicated checkpoints.

Figure 2 provides examples of the variety of security procedures and technologies used by TSA, airport operators, and air carriers at typical category X or I airports to control access to security-restricted areas of airports and help mitigate insider threats. These efforts vary by airport, local needs, and resources available, among other factors.

Figure 2: Examples of Security Procedures and Technologies Used by Transportation Security Administration (TSA) or Other Aviation Stakeholders to Help Mitigate Insider Threats at TSA-Regulated Airports



Source: GAO analysis of TSA data. | GAO-20-275

Note: TSA and aviation stakeholders may use other security procedures and technologies not depicted in this figure to mitigate insider threats. The location and use of security procedures and technologies varies by airport.

TSA Has Ongoing Efforts to Help Mitigate Insider Threats and Plans to Further Enhance Its Insider Threat Program

TSA's Long-standing Efforts that Help Mitigate Insider Threats

TSA has long-standing, established activities that the agency has conducted that help mitigate insider threats. These efforts directly or indirectly regulate or facilitate security at commercial airports and help mitigate insider threats. Specifically, TSA has programs to increase awareness of insider threats in the aviation community, analyze and disseminate intelligence, vet aviation workers and TSA staff, inspect and assess security at airports, and share information with the aviation community. We have previously reported on these efforts in our work on aviation security and perimeter and access control security at airports.[25]

- **Awareness and training.** TSA promotes awareness of insider threats to the aviation community and disseminates materials on how to identify and report insider threats to aviation stakeholders, which they may use on a voluntary basis.
- **Analyze and disseminate intelligence.** TSA evaluates intelligence information related to both domestic and international adversaries (such as terrorists) who seek to leverage insiders and target the U.S. transportation system, among other things. TSA regularly disseminates this information to aviation stakeholders through TSA's intelligence officers at its field offices, for example. There are approximately 80 field intelligence officers stationed throughout the U.S., Puerto Rico, and Guam, who provide information to airport officials and the aviation community on insider tactics and emerging threats, among other things.
- **Vetting aviation workers.** TSA facilitates background checks of aviation workers (e.g. baggage handlers and concessionaire employees) applying for unescorted access to security-restricted areas of airports. The background check includes a Security Threat Assessment that is generally made up of three parts: (1) near real-time vetting against terrorism watch lists and other federal databases, (2) verification of the applicant's lawful presence in the United States, and (3) a fingerprint-

[25]GAO, *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeter and Access Controls*, GAO-09-399 (Washington, D.C.: Sept. 30, 2009). GAO, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*, GAO-16-632 (Washington, D.C.: May 31, 2016).

based criminal history records check.[26] Additionally, TSA staff, such as transportation security officers, undergo a pre-employment screening, including all parts of the Security Threat Assessment and other security checks, and a background investigation to determine the applicant's suitability for the position.[27] Depending upon their job duties, TSA staff at airports may be issued credentials for unescorted access to security-restricted areas of an airport.

- **Inspections and assessments.** Staff at TSA compliance hubs (field offices) inspect airports and air carriers and test security measures to ensure compliance with federal requirements. To further enhance airport security, TSA also performs comprehensive, targeted, and supplemental inspections and other compliance activities, such as assessments, investigations, and tests.
- **Guidance, policies, and information sharing.** TSA issues guidance and policies that, among other things, require airport operators and air carriers to implement or enhance access controls or other security measures, or share best practices on improving security and mitigating insider threats. TSA regularly communicates with aviation stakeholders to discuss security issues and policies.

TSA's Recent Efforts to Mitigate Insider Threats

Since the beginning of fiscal year 2017, TSA has implemented a variety of activities to oversee and facilitate insider threat mitigation at commercial airports, either through new activities or by enhancing ongoing efforts. Among other things, TSA has taken steps to further augment vetting of aviation workers, enhance aviation worker screening, test airport security targeted toward identifying insider risks and

[26]TSA does not require aviation workers with air operations area-only access to undergo a fingerprint-based criminal history records check; however, according to TSA officials, some airport operators do.

[27]Pre-employment screening for TSA staff includes other security checks, such as checking whether the applicant has previously applied for employment with the Department of Homeland Security and checking the applicant's credit history. This practice also applies to the screening personnel of private contractors participating in TSA's Screening Partnership Program, whereby private sector companies contract with TSA to provide screening services at TSA-regulated airports. See 49 U.S.C. § 44920.

vulnerabilities, and develop reference tools and guidance.[28] See below for examples of TSA's insider threat mitigation efforts initiated since the beginning of fiscal year 2017.

Additional Vetting Efforts

- **Social media analysis.** TSA augmented the vetting process for aviation workers, described above, in 2018 to include an evaluation of publically available social media information for individuals who match against a federal watch list and are applying for unescorted access to security-restricted areas of an airport.[29] TSA uses information about the individual, including the social media information, to conduct the security threat assessment and determine whether to approve or deny the application.
- **Proposed requirement for Rap Back enrollment.** The Federal Bureau of Investigation's Rap Back Service provides participating entities with ongoing notification of subsequent criminal activity that occurs after an individual's initial criminal history records check. In 2019, TSA proposed requiring airport operators and air carriers to enroll in Rap Back and to subscribe covered aviation workers.[30] As of December 2019, TSA has not yet imposed this requirement.[31]

[28]Some of these actions have been in response to provisions of recently enacted statutes. For example, the Aviation Security Act of 2016 required TSA to increase the number of covert tests of access controls to any secure area of the airport. See Pub. L. No. 114-190, tit. III, subtit. D, § 3408, 130 Stat. 615, 661 (2016) (enacted on July 15, 2016, as part of the FAA Extension, Safety, and Security Act of 2016). The TSA Modernization Act required TSA to ensure that, consistent with the Aviation Security Act of 2016, the TSA-led, random employee physical inspection efforts of aviation workers are targeted, strategic, and focused on providing the greatest level of security effectiveness. See Pub. L. No. 115-254, div. K, tit. I, § 1934(g), 132 Stat. 3186, 3573 (2018) (enacted on October 5, 2018, as part of the FAA Reauthorization Act of 2018).

[29]For example, aviation workers are vetted against the Terrorist Screening Database, which is, in general, the federal government's consolidated watch list of known and suspected terrorists.

[30]Airport operators and air carriers have been able to voluntarily enroll in Rap Back since October 2016, and as of November 29, 2019, 183 airport operators and six air carriers had enrolled in Rap Back.

[31]For example, TSA may require that regulated entities, such as airport operators and air carriers, adopt national amendments to their security programs if it determines the measures contained in such an amendment are needed.

Physical Screening of Aviation Workers

- **Advanced Threat Local Allocation Strategy (ATLAS).** TSA's ATLAS tool generates a randomized schedule and location of procedures to physically screen aviation workers. The ATLAS tool randomly identifies the type of screening procedure by balancing on-person screenings, such as pat-down searches, and in-property screenings, such as testing for traces of explosives on workers' property. Federal security directors may tailor the screenings and location based on local intelligence. TSA started using ATLAS in 2018 at high-risk airports to screen aviation workers entering or within security-restricted areas.

Testing and Vulnerability Assessments

- **Covert testing.** TSA's covert testing teams help identify security vulnerabilities in multiple aspects of aviation security (including airport access controls and vulnerabilities to insiders) and may recommend additional measures or procedures be implemented to mitigate these vulnerabilities.[32] As described above, TSA increased the number of covert tests related to airport access controls and insider vulnerabilities in response to provisions of the Aviation Security Act of 2016. Further, in 2019, TSA began a covert test to assess vulnerabilities in TSA's ATLAS program.
- **Joint Vulnerability Assessment.** Joint teams of TSA and Federal Bureau of Investigation officials assess vulnerabilities in multiple aspects of airport security and operations including fuel, cargo, catering, general aviation, terminal area, and law enforcement operations. The assessments are conducted at commercial airports identified as high-risk every three years and on a case-by-case basis at other airports.[33] TSA revised the joint vulnerability assessment process in fiscal year 2017 to identify insider threat vulnerabilities and to suggest options to mitigate them.
- **Insider Threat Mitigation Activity.** In addition to the regular airport inspection and assessment duties, starting in fiscal year 2017, TSA required its aviation transportation security inspectors to conduct unannounced tests related to mitigating insider threats every fiscal year.

[32]TSA defines a covert—or undercover—test at domestic airports as any test of security systems, personnel, equipment, or procedures to obtain a snapshot of the effectiveness of airport passenger security checkpoint screening, checked baggage screening, airport access control, or other aviation security measures to improve performance, safety, and security.

[33]See 49 U.S.C. § 44904; Pub. L. No. 104-264, § 310, 110 Stat. 3213, 3253 (1996).

Guidance, Notice, and Information Sharing

- **Fraudulent identification guidance.** In fiscal year 2017, TSA developed guidance for airport operators and air carriers on detecting fraudulent identification documents, including methods for detecting fraudulent identification and appropriate responses when discovered.
- **Security directives.** TSA updated a security directive in 2018 to mitigate potential insider threats by, among other things, requiring airport operators to post signs at sterile area entry points accessible by credentialed aviation workers.[34] These signs advise individuals that they may be subject to inspection, among other things. Additionally, airport operators are required to conduct random inspections of vehicles when entering secured areas.
- **Information Circulars.** TSA issued information circulars in 2018 and 2019 that (1) recommended that airport operators and air carriers with exclusive area agreements conduct a vulnerability assessment of insider risks and develop a risk mitigation plan, and included best practices for the mitigation plan, and (2) described measures to prevent unauthorized access to aircraft and the flight deck.[35]

Efforts to Enhance the Insider Threat Program

TSA has implemented efforts aimed toward enhancing its Insider Threat Program. TSA established an Executive Steering Committee with members from the program's key offices to provide executive support and oversight across the multiple offices that compose the program. Also, TSA's Insider Threat Advisory Group collaborated with the Aviation Security Advisory Committee (ASAC) to review and develop recommendations that would address gaps, redundancies, and vulnerabilities in the program.

- **TSA Insider Threat Executive Steering Committee.** TSA established the Steering Committee in October 2018 to be the central oversight body for managing insider risks and coordinating the agency's mitigation strategies. Its purpose is to facilitate collaboration and decision-making across the program's multiple offices, advance an integrated agency-wide strategy, and establish consistent executive support for TSA and ASAC efforts, among other things. Its work to date includes reviewing the

[34]TSA Security Directive 1542-18-01A, December 6, 2018.

[35]TSA Information Circular 15-01E, August 30, 2018; TSA Information Circular 19-01, February 28, 2019.

2019 ASAC recommendations described above and approving the development of the Insider Threat Roadmap, which is to describe TSA's strategic vision.

- **TSA *Administrator's Intent* initiatives.** Several objectives and initiatives from the *Administrator's Intent,* published in June 2018, relate to mitigating insider threats.[36] It identifies specific priorities, strategic goals, and objectives that the Administrator plans to accomplish by 2020. For example, one objective is to modernize TSA's Insider Threat Program by, among other initiatives, expanding the Insider Threat Unit with dedicated staff from several key TSA offices.
- **ASAC Subcommittee on Insider Threats.** In 2018, the ASAC established a permanent, joint industry-government Subcommittee with members from TSA and various aviation stakeholders. The purpose of the Subcommittee is to provide a holistic and sustained body to research and make recommendations on risks posed by aviation workers to harm the aviation system. Previously, ASAC convened an industry-only Working Group on Airport Access Control on an as-needed basis.
- **ASAC recommendations.** In May 2019, at the request of the TSA Administrator, the ASAC issued a report to help enhance and broaden TSA's Insider Threat Program through 21 recommendations. The recommendations span six areas of the insider threat concept:
    1. threat detection, assessment, and response;
    2. aviation worker vetting and evaluation;
    3. aviation worker screening and access control;
    4. training and engagement;
    5. information sharing; and
    6. governance and internal controls.

  TSA concurred with all 21 of the recommendations. As of October 2019, TSA officials reported that the agency had implemented one of the recommendations and created a document that details implementation steps for the remaining 20, progress on those implementation steps, and estimated timeframes for completion. According to TSA officials, previous recommendations made by ASAC have significantly contributed to the establishment and development of the Insider Threat Program, and they anticipate the 2019 report's recommendations will have a similar positive

[36]Transportation Security Administration, *Administrator's Intent* (June 1, 2018).

effect.[37] Further, TSA officials said that the next iteration of the *Administrator's Intent* will incorporate these ASAC recommendations to help ensure that their implementation is tracked at the enterprise level.

Many Airport Operators Reported Screening Workers, Using Access Controls, and Providing Training that Exceed Regulatory Requirements and Help Mitigate Insider Threats

Overall, many airport operators help ensure the security of their facilities, including mitigating insider threats, through their efforts to comply with TSA regulations. However, airport operators may also implement additional measures beyond those required by TSA to improve their security posture. Some examples of voluntary efforts airport operators have reported implementing to help mitigate insider threats include physical screening of aviation workers at access points to SIDAs or secured areas in addition to TSA's random screening under the ATLAS program, using sophisticated access control technologies such as biometric fingerprint readers, and offering or requiring training for aviation workers on additional security awareness topics.

Aviation Worker Screening

Although TSA requires airport operators to perform random aviation worker screening at sterile area access points, it does not require them to physically screen all aviation workers at all access points to security-restricted areas, at all times.[38] However, some airport operators choose to voluntarily implement screening programs to physically search some or all workers or their property as they enter security-restricted areas.

[37]See recommendations in the Aviation Security Advisory Committee's report to TSA, Aviation Security Advisory Committee, *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control* (April 8, 2015). In this 2015 report, ASAC provided 28 recommendations to TSA to help mitigate insider threats at commercial airports. TSA concurred with all 28 recommendations and have since closed 25 of these recommendations. The remaining three recommendations required longer-term solutions, and TSA decided to incorporate this work into their efforts to address ASAC's 2019 recommendations.

[38]Aviation workers who only require access to the sterile area, such as concessionaires, must pass through the TSA passenger screening checkpoint if their access media credentials do not permit them access through other entry points to the sterile area.

According to our analysis of TSA data collected in July through September 2019 from a representative sample of airports on their current insider threat mitigation measures, seven of 27 category X airports' officials and 13 of 54 category I airports' officials reported that when they screen aviation workers passing through an access point, they screen 100 percent of workers, their property, and their vehicles (if the screening operations take place at a vehicle access point). Airport officials from four of 44 sampled category II airports, 10 of 54 sampled category III airports, and one of 58 sampled category IV airports reported that they screen 100 percent of workers when screening operations are underway.[39]

At one category X airport we visited, airport officials said they implemented full worker screening, following the lead of one tenant air carrier. According to the officials, the airport has two worker screening checkpoints in the publicly-accessible baggage claim area that are used by all workers entering the security-restricted areas. These checkpoints use X-ray machines, explosives trace detection, and walk-through metal detectors to screen aviation workers and their property and ensure they do not carry items that are otherwise prohibited (e.g. firearms and illicit substances) and not required to perform their work duties beyond the worker checkpoint. Airport officials said these checkpoints are staffed by a dedicated crew of screeners employed by the airport operator, and officials believe having a consistent crew over time makes it easier for screeners to detect if a worker is behaving in an uncharacteristic or suspicious way.

At one category I airport we visited, officials said that they established an insider threat program and implemented measures to mitigate insider threats in response to an illegal drug smuggling operation involving aviation workers that occurred at their airport. For example, they partner with TSA and local law enforcement to conduct full worker screening operations two to three times per week at randomly-selected times and locations, which supplements TSA's ATLAS operations. Officials said during these operations, all arriving workers are funneled to the screening

[39]According to Security Directive 1542-18-01A, airport operators are required to conduct random inspections of individuals entering the sterile area at entry points other than the screening checkpoints to verify that they have appropriate and valid ID and access control media, and to determine if they are carrying prohibited items other than those required for operational needs. The inspections must be clearly visible to other individuals exercising their access privileges. The rate and locations of random inspections must be approved by the federal security director and must be significant enough such that there is a reasonable expectation that individuals exercising their access privileges will be subject to an inspection.

locations, and they are directed to walk through screening equipment that is capable of identifying metallic threats (e.g. guns and knives) and non-metallic threats (e.g. suicide vests and other weapons) both on person and in property. If the machines are not used, airport officials coordinate with TSA to conduct full-body pat-downs of all employees. Airport officials may also use open-and-look bag searches. At the same time, local law enforcement patrols the screening area with canine units to search for drugs and explosives.

Access Control Technology at Airports

In general, category X, I, II, and III airports are required to implement measures to control access and prevent unauthorized entry to security-restricted areas of the airport. Airports choose their specific access control system and technology, such as cipher or keyed locks, proximity swipe cards, PIN readers, and biometric (e.g. fingerprint) authentication, provided such technology meets the standards of their TSA-approved security program. Category IV airports—which are typically the smallest commercial airports—are generally not required to identify security-restricted areas within their security programs and thus may not have mechanisms in place to control access to such areas.[40] However, like the larger commercial airports, security programs for category IV airports must provide for adequate law enforcement support, and airport operators at these airports may choose to establish security-restricted areas and

[40]Unless implementing a complete or enhanced supporting security program, as described earlier in this report, airport operators of category IV airports generally would not have designated security-restricted areas as part of their security programs. According to TSA, an enhanced supporting program, which is implemented by some category IV airports, includes some but not all elements of a complete security program beyond what is required of the supporting security program. However, TSA is required by law to ensure that all passengers and property departing on aircraft from a TSA-regulated airport are screened and pursuant to federal regulations, air carriers remain ultimately responsible for ensuring that individuals have been adequately screened before permitting them to board an aircraft. See 49 U.S.C. § 44901(a); 49 C.F.R. § 1544.207.

implement access control technologies or other measures at their discretion.[41]

According to our analysis of TSA data collected in July through September 2019 from a representative sample of airports, officials from most category X, I, and II airports reported that they have systems that use more than one technology to control access to sterile and secured areas of the airport, as shown in figure 3.[42] Among category III airports, officials from 27 of 54 also reported using multiple technologies. Among category IV airports, officials from 37 of 58 reported using some type of access control technology, the most common being locks and keys.

[41]According to TSA officials, security regulations are designed to provide varying levels of protection based upon the size, type, and frequency of aircraft operations. They said that security measures, therefore, are more demanding at airports where air carriers utilize large transport airplanes with 61 or more seats, and have scheduled departures and arrivals. Airports served only by smaller aircraft with 60 or fewer seats and that do not enplane from or deplane into a sterile area need not comply with all requirements appropriate for airports served by larger aircraft. See 49 C.F.R. § 1544.101(a)(2). According to TSA officials, this approach, first implemented by Federal Aviation Administration in 1981 and currently maintained by TSA, allows smaller airports to implement security measures in a more economical manner and provides an acceptable level of security. However, TSA issued Information Circular 19-02 in June 2019 in an effort to raise the security baseline at airports with partial and supporting security programs by recommending voluntary security best practices to mitigate potential vulnerabilities that could allow an individual to introduce weapons or explosive devices onto aircraft.

[42]The data does not include the technologies used to control access to the sterile area through passenger screening checkpoints.

Figure 3: Number of Airports Reporting Employing Access Control Technologies at the Majority of Access Points Used by Aviation Workers to Access Secured or Sterile Areas, by Airport Category

	X	I	II	III	IV
 Lock and key	0	0	0	2	20
 Proximity badge reader	1	3	13	23	10
 Proximity badge reader +  PIN pad	16	41	24	23	6
 Proximity badge reader +  PIN pad +  Fingerprint reader	10	10	7	4	1
Total number of sampled airports	27	54	44	54	58

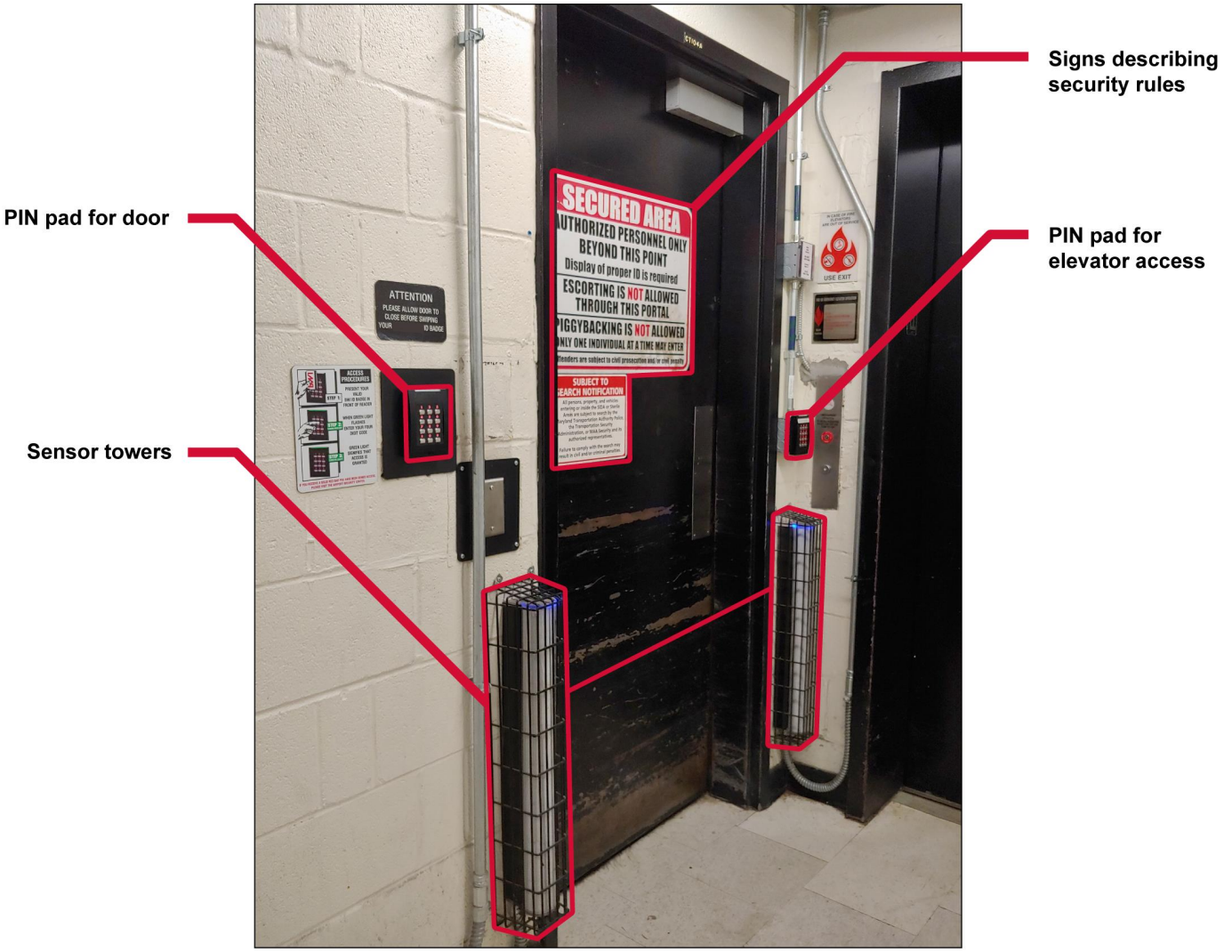
Source: GAO analysis of TSA data. | GAO-20-275

Note: Source data were collected by TSA from a representative sample of airports in July-September 2019 via an electronic questionnaire. Access points are doors (and sometimes vehicle access gates) that are accessible to aviation workers with unescorted access to security-restricted areas, such as secured or sterile areas. Secured areas are areas for which security measures, such as access controls, must be carried out to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles. This includes areas where domestic and foreign air carriers enplane and deplane passengers and sort and load baggage, and any adjacent areas not separated by adequate security measures. Sterile areas are areas that, in general, provide passengers access to boarding aircraft and to which access is controlled through the screening of passengers and property. Most (but not all) category IV airports operate under supporting or partial airport security programs, which do not require that airport operators establish sterile or secured areas or personnel identification media systems.

Technology at two category X airports we visited is used specifically to prevent workers from “piggybacking,” or attempting to enter security-

restricted areas by following close behind another worker without swiping a proximity card or entering a PIN for access. For example, one airport has sensor towers at high-traffic doors from unsecured to secured areas of the airport. The two towers—one on each side of the door—can detect if more than one person crosses the threshold after only a single proximity card swipe and PIN entry. According to airport officials, when this happens, the nearby security cameras will pan toward the door so that security officials who monitor the feeds can view the individuals at the door and respond appropriately. Figure 4, below, shows this technology, as well as the proximity card reader and PIN pad, a separate reader and pad for elevator access, and signs describing security rules.

Figure 4: Access Control Technologies at an Access Point to a Secured Area of an Airport

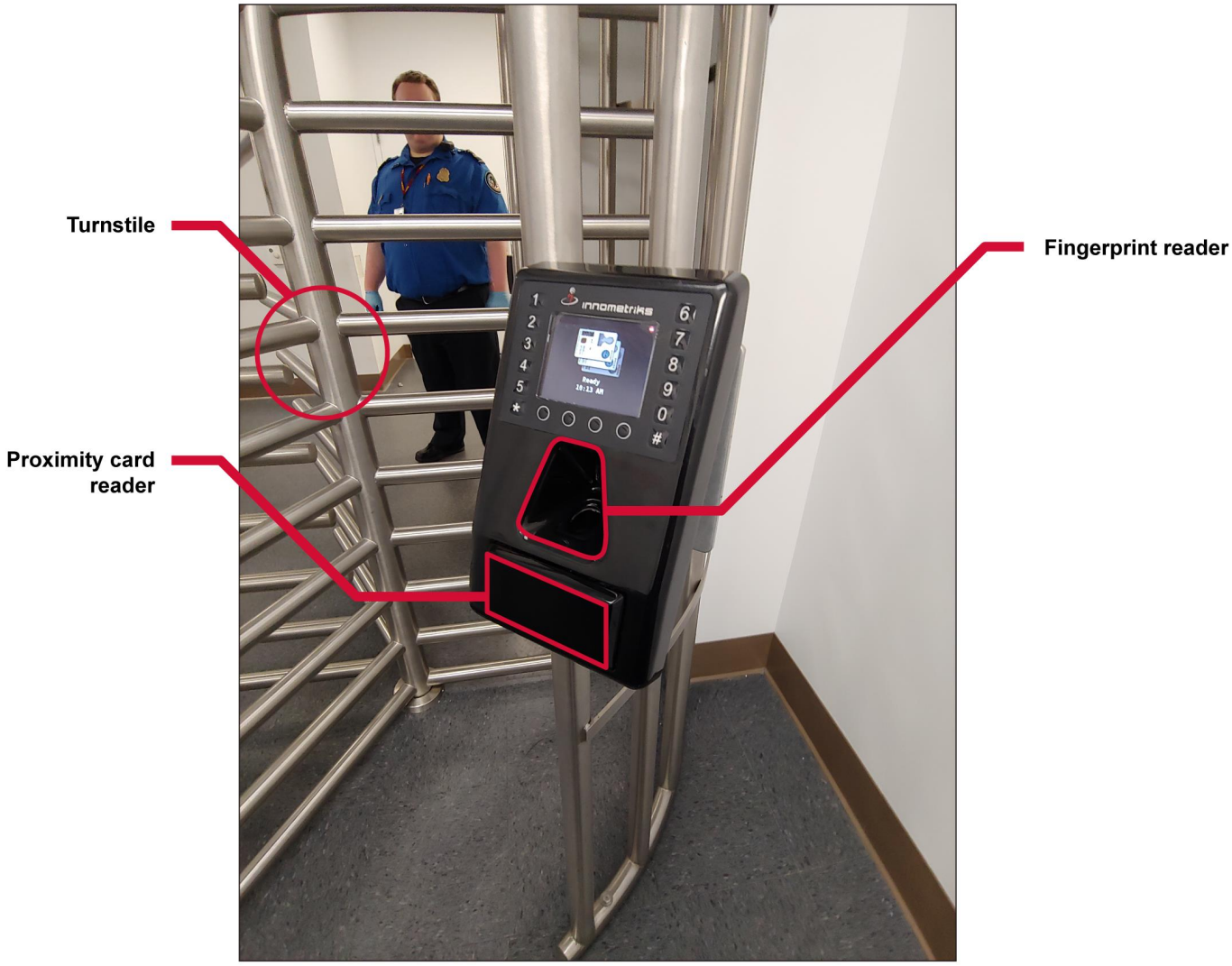


Source: GAO. | GAO-20-275

Note: Access points are doors (and sometimes vehicle access gates) that are accessible to aviation workers with unescorted access to security-restricted areas, such as secured or sterile areas. Secured areas are those areas for which security measures, such as access controls, must be carried out to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles. This includes areas where domestic and foreign air carriers enplane and deplane passengers and sort and load baggage, and any adjacent areas not separated by adequate security measures.

At a second category X airport we visited, locking turnstiles are used to prevent piggybacking. Each worker who wishes to go through the access point must present their proximity badge and provide a fingerprint. Only then will the locked turnstiles unlock to allow that worker through. The turnstiles are on a timer, so if a worker does not go through within a set time, they will have to repeat the process from the beginning. Additionally, if a badge is presented more than one time within a specified time period, an alarm is triggered in the Airport's Security Operations Center to alert airport security staff of a potential piggybacking incident. Figure 5 shows the card reader, fingerprint reader, and turnstile in use at one access point. Behind the turnstile, a TSA agent conducting ATLAS countermeasures waits for workers to come through.

Figure 5: Access Control Technologies at an Access Point to a Secured Area of an Airport



Source: GAO. | GAO-20-275

Note: Access points are doors (and sometimes vehicle access gates) that are accessible to aviation workers with unescorted access to security-restricted areas, such as secured or sterile areas. Secured areas are those areas for which security measures, such as access controls, must be carried out to prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles. This includes areas where domestic and foreign air carriers enplane and deplane passengers and sort and load baggage, and any adjacent areas not separated by adequate security measures.

Training

In general, according to TSA requirements, individuals with unescorted access to security-restricted areas of category X, I, II, and III airports must be trained on, among other things, escort procedures and the display and use of identification media. All airport operators across all airport categories must ensure that training for law enforcement personnel addresses the airport's security program, among other security-related topics.

For training offerings beyond what is required by TSA, our analysis of TSA data collected in July through September 2019 from a representative sample of airports showed the majority of airport operators at category X, I, II, and III airports reported that they offered or required training for aviation workers that specifically discusses insider threats, as shown in Table 2.[43]

Table 2: Number of Airport Operators Reporting Offering or Requiring Training for Aviation Workers on Insider Threats, by Airport Category

Category	X (airport category)	I (airport category)	II (airport category)	III (airport category)	IV (airport category)
Offers or requires Insider Threat training	25	49	38	42	20
Does not offer or require Insider Threat training	2	5	6	12	38
Total number of sampled airports	**27**	**54**	**44**	**54**	**58**

Source: GAO analysis of TSA data. | GAO-20-275

Note: Source data were collected by TSA from a representative sample of airports in July-September 2019 via an electronic questionnaire. TSA classifies the nation's approximately 430 TSA-regulated airports into one of five categories (X, I, II, III, and IV) based on various factors, such as the number of take-offs and landings annually, the extent of passenger screening at the airport, and other security considerations. In general, category X airports have the highest number of passenger enplanements and category IV airports have the fewest. An "aviation worker" is an employee, contractor, or representative of an airport operator, U.S. or foreign-flagged (i.e., domestic or foreign) air carrier, vendor, concessionaire, tenant, government agency (including TSA), entity in the air cargo supply

[43]For example, airport operators may not authorize any individual unescorted access to the SIDA unless they have successfully completed training in accordance with a TSA-approved curriculum specified in the airport's security program. See 49 C.F.R. § 1542.205(b). Such curriculum must include discussions of the unescorted access authority of the individual, control, use, and display of access and identification media, escort and challenge procedures, security responsibilities outlined in 49 C.F.R § 1540.105, and restrictions on divulging sensitive security information, which is protected from unwarranted disclosure in accordance with 49 C.F.R. part 1520. See 49 C.F.R. § 1542.213(b).

chain, or other entity who may at any time work or conduct operations at an airport or areas adjacent to or connected with an airport (including an entity's supply chains) subject to regulation by TSA.

Moreover, although they are not required to do so by TSA, many category IV airports reported they offer or require training on a variety of security-related topics, such as insider threats and reporting suspicious behavior and unusual activity.

Air Carriers in Our Review Reported Mitigating Insider Threats by Complying with TSA Requirements, and Some Reported Supplementing Their Efforts

The six air carriers we spoke with reported they mitigate insider threats via their efforts to comply with federal requirements through their TSA-approved security programs.[44] In general, federal regulations require that air carriers employ a variety of procedures to mitigate security threats. Among others, these measures may include:

- Preventing unauthorized access to security-restricted areas over which they have primary responsibility, such as aircraft (e.g. by performing regular searches) and areas covered by an exclusive area agreement, as applicable;[45]
- Submitting applicant biographic information for criminal history records checks prior to issuing air carrier identification media or recommending that airport operators issue access credentials that grants an individual unescorted access to security-restricted areas of the airport;
- Using personnel identification systems that track information such as identification media expiration dates and appropriate level of access; and
- Providing training for workers who perform security-related duties or otherwise require access to security-restricted areas.

Air carriers may also choose to voluntarily implement additional efforts to improve their security posture. As described above, these may be incorporated into an individual air carrier's security program, but not necessarily. Air carriers we spoke with have implemented a variety of security measures. For example:

- To prevent unauthorized access to secured areas included in their exclusive area agreement or within their operations area, all air carriers

[44]We selected six of the largest U.S.-based carriers based on revenue generated over a 12-month period, as identified by the Department of Transportation Bureau of Transportation Statistics.

[45]See 49 C.F.R. § 1542.111.

we spoke to said they secure their facilities by employing at least one form of access control technology. The majority of air carriers (five of six) reported that they secure most access points with proximity card or fob readers, including one air carrier that reported it secures its access doors using additional measures beyond a proximity card swipe, requiring a PIN and a fingerprint as well. The sixth air carrier we spoke to said workers access security-restricted areas using keys or cipher combinations.

- Prospective air carrier employees may require access media credentials from the airport operator in addition to the air carrier. In some cases, the air carrier will accept the criminal history records check conducted by the airport operator to issue its own credentials, but officials from some air carriers we spoke to said they conduct more rigorous checks before issuing their air carrier credentials. For instance, one air carrier reported that it checks both the applicant's employment history in addition to their criminal history, and it uses an additional set of disqualifying criteria beyond the regulatory minimum to determine suitability for hire.[46]

Some air carriers choose to further enhance their insider threat mitigation efforts. For example, one air carrier has a dedicated insider threat program and, at 16 airports, it implemented a screening program of workers and their belongings at dedicated checkpoints. Another air carrier created a team to monitor the use of the Known Crewmember program, a screening program that provides flight and cabin crews with expedited screening that may include a dedicated screening lane. According to air carrier officials, at its largest hub airport, the team reports on workers from all air carriers who violate the program's rules to TSA. Some examples of such violations include crewmembers using the dedicated lane for leisure international travel or carrying other individuals' bags through the Known Crewmember portal or passenger screening checkpoint and into sterile areas of the airport.

[46]An individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the 28 disqualifying criminal offenses listed in 49 C.F.R § 1544.229(d) in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority or while the individual has unescorted access authority. See 49 C.F.R. § 1544.229.These offenses include, but are not limited to, interference with air navigation, aircraft piracy, murder, espionage, armed or felony unarmed robbery, and conspiracy or attempt to commit any of the criminal acts listed in paragraph (d).

TSA's Insider Threat Program is Not Guided by a Strategic Plan with Goals and Objectives, nor Performance Goals to Assess Program Performance

TSA's Insider Threat Program Does Not Have a Strategic Plan with Goals and Objectives

Although TSA has multiple ongoing efforts to mitigate insider threats at commercial airports carried out by a number of offices, it does not have a strategic plan in place to guide its Insider Threat Program. When the program began in 2013, TSA initially developed a 2014-2016 Insider Threat Action Plan, which described TSA's vision of an integrated insider threat program at TSA, and it included strategic goals, each with a set of objectives. However, according to TSA officials, TSA did not fully implement this Action Plan, and TSA did not renew or revise the Action Plan after 2016 due to the departure of the key sponsoring senior leader. Further, TSA officials said that the Action Plan does not reflect all the existing activities that TSA's Insider Threat Program currently encompasses because the program has changed since 2014.

TSA is aware of the importance of strategic planning and took steps to strategically plan for other programmatic efforts at the agency. For example, in 2019, TSA revised its *National Strategy for Airport Perimeter and Access Control Security.*[47] This strategy describes how TSA seeks to secure the perimeter and control access to security-restricted areas of U.S. commercial airports, which is one concern related to insider threats. In 2018, TSA published its *Administrator's Intent* to outline how TSA planned to execute its agency-wide strategy in the short term.[48] The *Intent* includes one strategic objective to modernize elements of TSA's Insider Threat Program, such as vetting capabilities. Also in 2018, TSA published the *Cybersecurity Roadmap 2018,* which details the agency's efforts to protect its information technology infrastructure from adversaries who

[47]Transportation Security Administration, *National Strategy for Airport Perimeter and Access Control Security* (January 3, 2019).

[48]Transportation Security Administration, *Administrator's Intent* (June 1, 2018).

might seek to cause harm.[49] Each of these documents contains the critical elements of strategic plans that are laid out by the Office of Management and Budget, including strategic goals and objectives. These strategic planning documents contain elements related to insider threats and can be drawn upon to help develop a comprehensive strategic plan that encompasses the myriad of activities across its many offices that compose TSA's Insider Threat Program.

In October 2018, TSA established the Insider Threat Executive Steering Committee in an effort to establish consistent executive-level engagement and support from the agency's senior management. As described above, TSA's Insider Threat Program is carried out by multiple, distinct offices at TSA, and TSA officials have indicated that the program could benefit from a more cohesive approach and oversight. During the course of our review, the Steering Committee approved the development of an Insider Risk Roadmap (Roadmap). According to TSA officials, the Roadmap is under development as of January 2020, and when completed, is to describe the future of insider risk mitigation for TSA. TSA officials were uncertain, however, of when the Roadmap would be completed and implemented. Given that TSA did not fully implement its 2014-2016 Insider Threat Action Plan, and it was never renewed or revised, it is important that TSA remain committed to developing and implementing the Roadmap and, as it moves forward in drafting the Roadmap, ensuring that it contains the critical elements of a strategic plan, including strategic goals and objectives.

Federal internal control standards establish that management should define the entity's objectives clearly and in alignment with the entity's mission and strategic plan. Objectives should specifically identify what is to be achieved, how, by whom, and in what time frame, and should be defined in measurable terms so that performance toward achieving such objectives can be assessed consistently.[50] More specifically, the Office of Management and Budget clarifies that a strategic goal articulates clearly what the agency wants to achieve to advance its mission, while strategic objectives reflect the outcome or impact the agency is trying to achieve and should facilitate prioritization and assessment for planning,

[49]Transportation Security Administration, *TSA Cybersecurity Roadmap 2018* (November 1, 2018).

[50]GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G (Washington, D.C.: Sept. 10, 2014).

management, reporting, and evaluation. For example, mission-focused strategic objectives express specifically the path an agency plans to follow to achieve or make progress on a single strategic goal.[51]

Having a strategic plan for its Insider Threat Program would better position TSA to ensure it is effectively coordinating across its multiple offices and leveraging each office's resources to mitigate insider threats, a threat which has consistently been identified as the second-highest enterprise level risk. A strategic plan, such as the ones included in other examples of TSA roadmaps, would help both to (1) link these individual efforts to the program's strategic goals and (2) describe how they contribute to the achievement of those goals and the agency's stated mission. TSA officials agreed that developing and implementing a strategic plan such as the ones associated with other roadmaps would help ensure that (1) its efforts to develop the Insider Threat Roadmap would continue to progress and (2) executive-level support for strategic planning would remain a priority.

TSA Does Not Have Performance Goals to Assess Its Insider Threat Program

Individual TSA offices have made progress developing methods to assess their individual office's efforts, but TSA does not have a comprehensive set of performance goals that can be used to assess progress toward achieving the Insider Threat Program's stated mission. The National Insider Threat Task Force, established under Executive Order 13587 of October 7, 2011, outlined the minimum standards and basic elements of an insider threat program as well as a Maturity Framework to help Executive Branch departments and agencies, such as TSA, increase the effectiveness of their insider threat programs, among other things.[52] According to the Framework, program senior officials should use metrics to represent progress and better articulate the central role of its insider threat program in achieving the department or agency's strategic objectives. The Office of Management and Budget specifies that

[51]Office of Management and Budget, *Preparation, Submission, and Execution of the Budget*, OMB Circular A-11 (revised July 2016).

[52]See Exec. Order No. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011, 76 Fed. Reg. 63,811 (Oct. 13, 2011); National Insider Threat Task Force, *Insider Threat Program Maturity Framework* (Washington, D.C.: November 1, 2018).

performance goals are statements of the desired performance target to be accomplished within a certain timeframe, and a suite of performance goals should be used to assess progress toward achieving each strategic objective. Federal standards for internal control also state that entities should use performance goals to evaluate their performance in achieving their strategic objectives.[53]

Some TSA offices have developed indicators for measuring characteristics of their insider threat activities, but these do not exhibit the characteristics of performance goals as defined by the Office of Management and Budget. For example, TSA's Security Operations office developed Key Performance Indicators for its ATLAS operations, which are operational indicators for the TSA staff carrying out the countermeasures. These include that teams must screen a percentage of workers who pass through the checkpoint and must meet their assigned screening time allotment. However, operational indicators such as these do not include baselines and timeframes for completion, which are characteristics of performance goals as described by the Office of Management and Budget. Moreover, the Insider Threat Program is without a strategic plan, and as a result, these operational indicators cannot link back to a strategic objective or show progress achieving such an objective, as called for by the Office of Management and Budget guidance.

TSA identified the need to develop performance goals to assess its progress and effectiveness in its 2014-2016 Insider Threat Action Plan, which called for "a performance management system [that] monitors and measures [the] effectiveness of [the] insider threat program." According to officials, such a performance management system was never developed because of the departure of the key senior leader, as described above. Further, in its May 2019 report to the Administrator, ASAC recommended that TSA develop measures that assess the performance of its insider threat efforts. For example, ASAC recommended that TSA commission a comprehensive federally-funded research and development center to assist TSA in evaluating the performance of random or unpredictable aviation worker screening methods to mitigate insider threats. The report indicated that establishing measures of effectiveness and evaluating performance on such measures is "vital to proactive and effective insider threat management." TSA officials said that the planned Insider Risk Roadmap may include performance goals for the Insider Threat Program,

[53]GAO-14-704G.

in addition to strategic goals and objectives. However, previous examples of Roadmaps for TSA efforts did not include references to specific, measurable performance goals that can be used to represent progress via targets and timeframes. Moreover, as described above, TSA officials are still drafting the Roadmap and are uncertain when it will be issued.

Having documented and clearly defined performance goals that are linked to the program's overarching strategic goals and objectives would better position TSA to understand the effectiveness of its insider threat efforts. As a result, TSA would be able to reduce the likelihood of expending resources on efforts that are not meeting the program's stated mission. Focusing on the intended results of TSA's insider threat efforts can promote strategic and disciplined management decisions that are more likely to be effective because managers are better able to target areas most in need of improvement and to select appropriate levels of investment. TSA could determine the success of its strategies, adjust its approach when necessary, and remain focused on results. Further, agency accountability can be enhanced when both agency management and external stakeholders—such as Congress—can assess an agency's progress toward meeting its strategic goals. By developing such performance goals, TSA will better position itself to determine the Insider Threat Program's progress toward achieving its mission of deterring, detecting, and mitigating insider threats to the aviation sector.

Conclusions

TSA has consistently identified the insider threat among its highest enterprise-level risks and characterizes it as a significant and complex risk to aviation security. In the last ten years, TSA and aviation stakeholders have faced a consistent threat posed by insiders who used their access privileges and knowledge to commit criminal acts, such as drug smuggling, gun smuggling, theft, and attempted suicide bombing. Having an effective Insider Threat Program is critical to TSA's ability to mitigate the risk of insiders causing harm to the civil aviation system. Since establishing its Insider Threat Program in 2013, TSA has taken steps to strengthen its efforts to combat the insider threat such as by implementing a program to physically screen aviation workers at high-risk airports. However, responsibility for the Insider Threat Program is spread across multiple offices within TSA and has made it challenging to synchronize and integrate activities across each office's efforts. As of January 2020, TSA officials said that the Insider Threat Program does not have a strategic plan. However, officials said they are developing a new

strategic “roadmap” for the Insider Threat Program but are uncertain when it will be issued. Developing and implementing a strategic plan with strategic goals and objectives will help improve coordination across the program’s multiple offices and prioritize and focus TSA’s efforts to ensure that resources are targeted effectively.

Additionally, TSA has also not established performance goals to help assess its overall progress in achieving its Insider Threat mission. With specific performance goals tied to strategic objectives, TSA will have the necessary mechanism to assess the extent to which the program is achieving its objectives and overall mission. TSA has numerous efforts across the agency to address insider threats; and with performance goals, the program could assess progress, identify successes, gaps, and redundancies and prioritize and allocate resources effectively. When dealing with a program designed to keep the aviation system safe from criminal and terrorist acts, agency leaders and policy makers need to know how well the government is doing implementing its objectives. Establishing performance goals will help the agency and Congress assess the progress of the overall insider threat effort, target areas most in need of improvement, and select appropriate levels of investment.

Recommendations for Executive Action

We are making the following two recommendations to TSA:

- The TSA Administrator should develop and implement a strategic plan for its Insider Threat Program that includes strategic goals and objectives. (Recommendation 1)
- The TSA Administrator should develop performance goals for its Insider Threat Program that assess progress achieving the strategic objectives in the insider threat strategic plan. (Recommendation 2)

Agency Comments and Our Evaluation

We provided a draft of this report to the Department of Homeland Security (DHS) for comment. In written comments, which are included in appendix I, DHS concurred with our two recommendations and described steps it plans to take to implement them, including an estimated timeframe for completion. TSA also provided technical comments, which we incorporated as appropriate.

In response to our recommendations, DHS's letter notes that TSA is in the process of drafting the 2020 Insider Threat Roadmap, which will include strategic goals and objectives to guide TSA in its efforts to mitigate insider threats. The letter further explains that the Roadmap will include performance measures to assess TSA's progress achieving those strategic objectives. If fully implemented, these actions should address the intent of the recommendations.

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

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

Triana McNeil
Director, Homeland Security and Justice

Appendix I: Comments from the Department of Homeland Security

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

Homeland Security

January 29, 2020

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

Re: Management Response to Draft Report: GAO-20-275, "AVIATION SECURITY: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals"

Dear Ms. McNeil:

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

The Department is pleased to note GAO's recognition of the Transportation Security Administration's (TSA) previous and current initiatives to mitigate insider threats at the Nation's airports. Specifically, GAO recognized the contributions of TSA's Insider Threat Program as well as its activities including programs to increase awareness of insider threats in the aviation community, analyze and disseminate intelligence, vet aviation workers and TSA staff, and inspect and test security at airports.

As a leader in transportation security, TSA is committed to continuously improving its ability to mitigate insider threats while remaining adaptive and innovative in its response to evolving threats. TSA is also committed to maintaining strong partnerships across government and industry to face future challenges.

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.

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, CIA, CFE
Director
Departmental GAO-OIG Liaison Office

Attachment

2

Attachment: Management Response to Recommendations Contained in GAO-20-275

GAO recommended that the TSA Administrator:

Recommendation 1: Develop and implement a strategic plan for its Insider Threat Program that includes strategic goals and strategic objectives.

Response: Concur. As was noted in the draft report, TSA's Law Enforcement/Federal Air Marshal Service (LE/FAMS) is currently in the process of drafting the 2020 Insider Threat Roadmap. The Insider Threat Roadmap will provide a strategic vision to guide TSA and the transportation community in mitigating insider threats. Built on the expertise, leadership, and relationships TSA has developed to streamline processes, identify requirements and capabilities, and leverage partnerships to proactively mitigate risk, the Roadmap will delineate the Guiding Principles, Strategic Priorities, and corresponding objectives for TSA's overarching, cross-modal approach to insider threats moving forward.

The Roadmap will be delivered to the Insider Threat Executive Steering Committee for endorsement and planned implementation.

Estimated Completion Date: June 30, 2020

Recommendation 2: Develop performance goals for its Insider Threat Program that assess progress achieving the strategic objectives in the insider threat strategic plan.

Response: Concur. The Strategic Priorities and corresponding objectives set forth in the Insider Threat Roadmap, currently being developed by LE/FAMS, will contain associated performance measures to assess progress and effectiveness.

Estimated Completion Date: June 30, 2020

3

Appendix II: GAO Contact and Staff Acknowledgments

GAO Contact

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

Staff Acknowledgments

In addition to the contact named above, William Russell (Director), Kevin Heinz (Assistant Director), Winchee Lin (Analyst in Charge), Sarah Williamson, Benjamin Crossley, Dominick Dale, Daniel Gaud, Thomas Lombardi, and Amanda Miller made key contributions to this report.

Appendix III: Accessible Data

Data Table

Accessible Data for Figure 3: Number of Airports Reporting Employing Access Control Technologies at the Majority of Access Points Used by Aviation Workers to Access Secured or Sterile Areas, by Airport Category

Category	X (airport category)	I (airport category)	II (airport category)	III (airport category)	IV (airport category)
Lock and key	0	0	0	2	20
Proximity badge reader	1	3	13	23	10
Proximity badge reader plus PIN pad	16	41	24	23	6
Proximity badge reader plus PIN pad plus fingerprint reader	10	10	7	4	1
Total number of sampled airports	27	54	44	54	58

Agency Comment Letter

Accessible Text for Appendix I Comments from the Department of Homeland Security

Page 1

January 29, 2020

Ms. Triana McNeil

Director, Homeland Security and Justice

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

Re: Management Response to Draft Report: GAO-20-275, "AVIATION SECURITY: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals"

Dear Ms. McNeil:

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

The Department is pleased to note GAO's recognition of the Transportation Security Administration's (TSA) previous and current initiatives to mitigate insider threats at the Nation's airports. Specifically, GAO recognized the contributions of TSA's Insider Threat Program as well as its activities including programs to increase awareness of insider threats in the aviation community, analyze and disseminate intelligence, vet aviation workers and TSA staff, and inspect and test security at airports.

As a leader in transportation security, TSA is co1mnitted to continuously improving its ability to mitigate insider threats while remaining adaptive and innovative in its response to evolving threats. TSA is also committed to maintaining strong partnerships across government and industry to face future challenges.

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.

Page 2

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, CIA, CFE

Director

Departmental GAO-OIG Liaison Office

Attachment

Page 3

Attachment: Management Response to Recommendations

Contained in GAO-20-275

GAO recommended that the TSA Administrator:

Recommendation 1: Develop and implement a strategic plan for its Insider Threat Program that includes strategic goals and strategic objectives.

Response: Concur. As was noted in the draft report, TSA's Law Enforcement/Federal Air Marshal Service (LEIFAMS) is currently in the process of drafting the 2020 Insider Threat Roadmap. The Insider Threat Roadmap will provide a strategic vision to guide TSA and the transportation community in mitigating insider threats. Built on the expertise, leadership, and relationships TSA has developed to streamline processes, identify requirements and capabilities, and leverage partnerships to proactively mitigate risk, the Roadmap will delineate the Guiding Principles, Strategic Priorities, and corresponding objectives for TSA's overarching, cross- modal approach to insider threats moving forward.

The Roadmap will be delivered to the Insider Threat Executive Steering Committee for endorsement and planned implementation.

Estimated Completion Date: June 30, 2020

Recommendation 2: Develop performance goals for its Insider Threat Program that assess progress achieving the strategic objectives in the insider threat strategic plan.

Response: Concur. The Strategic Priorities and corresponding objectives set forth in the Insider Threat Roadmap, currently being developed by LEIFAMS, will contain associated performance measures to assess progress and effectiveness.

Estimated Completion Date: June 30, 2020

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through our website. Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. You can also subscribe to GAO's email updates to receive notification of newly posted products.

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, https://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on Facebook, Flickr, Twitter, and YouTube.
Subscribe to our RSS Feeds or Email Updates. Listen to our Podcasts.
Visit GAO on the web at https://www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact FraudNet:

Website: https://www.gao.gov/fraudnet/fraudnet.htm

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548