United States Government Accountability Office

Report to Congressional Requesters

May 2016

# AVIATION SECURITY

# Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates

# GAO Highlights

Highlights of GAO-16-632, a report to congressional requesters

## Why GAO Did This Study

Incidents of aviation workers using access privileges to smuggle weapons and drugs into security-restricted areas and onto planes has heightened awareness about security at commercial airports. TSA, along with airport operators, has responsibility for securing the nation's approximately 440 commercial airports.

GAO was asked to review TSA's oversight of airport perimeter and access control security since GAO last reported on the topic in 2009. This report examines, for airport security, (1) the extent to which TSA has assessed the components of risk and (2) the extent to which TSA has taken actions to oversee and facilitate security, among other objectives.

GAO examined TSA documents related to risk assessment and security activities; analyzed relevant TSA security event data from fiscal years 2009 through 2015; obtained information from TSA and industry association officials as well as from a nongeneralizable sample of 11 airports, selected based on factors such as size.

## What GAO Recommends

GAO is making six recommendations, including that TSA update its Risk Assessment of Airport Security, develop and implement a method for conducting a system-wide assessment of airport vulnerability, and update its *National Strategy for Airport Perimeter and Access Control Security*. DHS concurred with the recommendations and identified planned actions to address the recommendations.

View GAO-16-632. For more information, contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov.
.

May 2016

# AVIATION SECURITY

## Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates

## What GAO Found

The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) has made progress in assessing the threat, vulnerability, and consequence components of risk to airport perimeter and access control security (airport security) since GAO last reported on the topic in 2009, such as developing its *Comprehensive Risk Assessment of Perimeter and Access Control Security* (Risk Assessment of Airport Security) in May 2013. However, TSA has not updated this assessment to reflect changes in the airport security risk environment, such as TSA's subsequent determination of risk from the insider threat—the potential of rogue aviation workers exploiting their credentials, access, and knowledge of security procedures throughout the airport for personal gain or to inflict damage. Updating the Risk Assessment of Airport Security with information that reflects this current threat, among other things, would better ensure that TSA bases its risk management decisions on current information and focuses its limited resources on the highest-priority risks to airport security. Further, TSA has not comprehensively assessed the vulnerability—one of the three components of risk—of TSA-regulated (i.e., commercial) airports system-wide through its joint vulnerability assessment (JVA) process, which it conducts with the Federal Bureau of Investigation (FBI), or another process. From fiscal years 2009 through 2015, TSA conducted JVAs at 81 (about 19 percent) of the 437 commercial airports nationwide. TSA officials stated that they have not conducted JVAs at all airports system-wide because of resource constraints. While conducting JVAs at all commercial airports may not be feasible given budget and resource constraints, other approaches, such as providing all commercial airports with a self-vulnerability assessment tool, may allow TSA to assess vulnerability at airports system-wide.

Since 2009, TSA has taken various actions to oversee and facilitate airport security; however, it has not updated its national strategy for airport security to reflect changes in its Risk Assessment of Airport Security and other security-related actions. TSA has taken various steps to oversee and facilitate airport security by, among other things, developing strategic goals and evaluating risks. For example, in 2012 TSA developed its *National Strategy for Airport Perimeter and Access Control Security* (Strategy), which defines how TSA seeks to secure the perimeters and security-restricted areas of the nation's commercial airports. However, TSA has not updated its Strategy to reflect actions it has subsequently taken, including results of the 2013 Risk Assessment and new and enhanced security activities, among other things. Updating the Strategy to reflect changes in the airport security risk environment and new and enhanced activities TSA has taken to facilitate airport security would help TSA to better inform management decisions and focus resources on the highest-priority risks, consistent with its strategic goals.

This is a public version of a sensitive report that GAO issued in March 2016. Information that TSA deems "Sensitive Security Information" has been removed.

# Contents

Tables

## Figures

## Abbreviations

| | |
|---|---|
| AAAE | American Association of Airport Executives |
| ACI-NA | Airports Council International-North America |
| ADASP | Aviation Direct Access Screening Program |
| AIM | Airport Information Management |
| AOA | Air Operations Area |
| ASAC | Aviation Security Advisory Committee |
| ASC | Airport Security Coordinator |

| | |
|---|---|
| ASP | airport security program |
| ASSET | Airport Security Self-Evaluation Tool |
| ATSA | Aviation and Transportation Security Act |
| CARAT | Commercial Airport Resource Allocation Tool |
| CATA | Civil Aviation Threat Assessment |
| COMSETT | Compliance Security Enhancement Through Testing |
| DHS | Department of Homeland Security |
| FAA | Federal Aviation Administration |
| FAMS | Federal Air Marshal Service |
| FBI | Federal Bureau of Investigation |
| FSD | federal security director |
| FTE | full-time equivalent |
| GPRA | Government Performance and Results Act of 1993 |
| GPRAMA | GPRA Modernization Act of 2010 |
| HSPD | Homeland Security Presidential Directive |
| ID | identification |
| JVA | joint vulnerability assessment |
| NA | national amendment |
| NIPP | National Infrastructure Protection Plan |
| NSAPAC-WG | National Strategy for Airport Perimeter Access Control Working Group |
| OIG | Office of Inspector General |
| PARIS | Performance and Results Information System |
| PIDS | perimeter intrusion detection system |
| PPD | Presidential Policy Directive |
| SD | security directive |
| SIDA | security identification display area |
| SIRT | Security Incident Reporting Tool |
| SOP | Standard Operating Procedures |
| SPOT | Screening of Passengers by Observation Techniques |
| SSI | Sensitive Security Information |
| TSA | Transportation Security Administration |
| TSSRA | Transportation Sector Security Risk Assessment |
| VIPR | Visible Intermodal Prevention and Response |

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

May 31, 2016

Congressional Requesters

Recent events of individuals gaining unlawful access to commercial airports and stowing away on planes as well as events of aviation workers using access privileges to smuggle weapons and drugs into security-restricted areas and onto planes has heightened awareness about perimeter and access control security at commercial airports.[1] For example, in April 2014, a 15-year-old boy allegedly climbed a perimeter fence at San Jose's Mineta International Airport in California and stowed away in the wheel well of a plane flying to Hawaii. In December 2014, a baggage handler at Atlanta's Hartsfield-Jackson International Airport in Georgia allegedly used his airport-issued credentials to repeatedly smuggle loaded and unloaded firearms into the passenger boarding area for hand-off to an accomplice, who carried the firearms onto an airplane bound for New York. The Department of Homeland Security's (DHS) Transportation Security Administration (TSA) and the Federal Bureau of Investigation (FBI) have characterized the threat of rogue aviation workers who exploit their credentials, access, and knowledge of airport security procedures for personal gain or to inflict damage—referred to as

[1] For purposes of this report, "security-restricted area" is a general term that encompasses areas of a commercial airport, identified in an airport's Transportation Security Administration (TSA)-approved security program, for which access is controlled and limited and includes areas accessible to passengers who have passed through a security checkpoint; "commercial airport" refers to an airport in the United States operating under a TSA-approved security program in accordance with 49 C.F.R. part 1542 that, in general, regularly serves air carriers with scheduled passenger operations (also referred to as "TSA-regulated airports"); "airport security," unless otherwise indicated, refers specifically to airport perimeter and access control security and includes, for example, measures in place to prevent unauthorized entry onto airport grounds or into other security-restricted areas of a commercial airport; and "aviation workers" refers to any individuals employed at an airport who require access to areas not otherwise accessible by the general public (i.e., security-restricted areas), including individuals directly employed by the airport operator as well as individuals employed by retail, air carrier, maintenance, custodial, or other entities operating on airport property.

the insider threat—as one of aviation security's most pressing concerns.[2] TSA is the federal agency with primary responsibility for securing the nation's civil aviation system, including overseeing and facilitating U.S. airport and aircraft operator efforts to maintain and improve the security of perimeters and access controls, and applying measures to reduce risks posed by aviation workers at the nation's commercial airports.[3] For example, TSA, airports, and air carriers are all to apply measures that reduce the insider threat, and airport operators generally have direct day-to-day operational responsibility for the security of their perimeters and access to security-restricted areas within the airport.[4] TSA, in turn, is responsible for establishing minimum security measures and regulating the implementation of those measures by airport operators and other regulated entities to improve perimeter and access control security. Both airports and air carriers may voluntarily implement measures above and beyond TSA's minimum requirements. TSA's fiscal year 2015 appropriation amounted to approximately $7 billion, the majority of which supports the agency's aviation security activities, including passenger checkpoint and baggage screening, the Federal Air Marshal Service

[2] TSA and the FBI define the insider threat to include threats to all aspects of aviation security, including passenger checkpoint, baggage, cargo screening, access controls, perimeter security, and off-airport aviation-related operations and activities, among other things.

[3] Pursuant to the Aviation and Transportation Security Act (ATSA), which was signed into law shortly after the terrorist attacks of September 11, 2001, TSA assumed primary responsibility for implementing and overseeing security operations with the U.S. civil aviation system. See Pub. L. No. 107-71, 115 Stat. 597 (2001). In general, civil aviation includes all nonmilitary aviation operations, including scheduled and chartered air carrier operations, cargo operations, and general aviation, as well as the airports servicing these operations.

[4] Airport operators do not, however, have direct day-to-day operational responsibility for the security of areas delegated to a specific air carrier via an Exclusive Area Agreement, which is an agreement between the airport operator and an air carrier to assume responsibility for specified security measures in a portion of a security-restricted area pursuant to 49 C.F.R. § 1542.111. Airport operators are also not responsible for the screening of passengers and property, which is a function performed by TSA personnel or, at airports participating in TSA's Screening Partnership Program, personnel employed by private sector screening companies. See 49 U.S.C. §§ 44901, 44920.

(FAMS), issuing and enforcing aviation security regulations, incident management, and other activities.[5]

In 2009, we reported that TSA had implemented activities to assess risks to airport perimeter and access control security.[6] However, we found that TSA had not completed a comprehensive risk assessment that included all three elements of risk—threat, vulnerability, and consequence—as required by the National Infrastructure Protection Plan (NIPP).[7] We also found that TSA's efforts to enhance the security of the nation's airports had not been guided by a unifying national strategy that identified key elements, such as goals, priorities, performance measures, and required resources. We recommended, among other things, that TSA develop a comprehensive risk assessment of airport security, and milestones for its completion, and a national strategy for airport security that includes key characteristics, such as goals and priorities. TSA generally agreed with our findings and recommendations, and the recommendations were closed based on actions TSA took to address the recommendations.

You asked us to review TSA's oversight of airport perimeter and access control security. This report examines (1) the extent to which TSA has assessed the components of risk—threat, vulnerability, and consequence—related to commercial airport perimeter and access control security since 2009; (2) the extent to which TSA has taken actions since 2009 to oversee and facilitate airport perimeter and access control

[5] See Department of Homeland Security Appropriations Act, 2015, Pub. L. No. 114-4, 129 Stat. 39, 44-46 (2015); see also 161 Cong. Rec. H281 (daily ed. Jan. 13, 2015) (explanatory statement) (describing in more detail amounts appropriated to TSA).

[6] 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).

[7] DHS, *National Infrastructure Protection Plan* (Washington, D.C.: June 2006). DHS issued the NIPP in response to the Homeland Security Act of 2002, as amended, and Homeland Security Presidential Directive/HSPD-7 (Dec. 17, 2003). See Pub. L. No. 107-296, § 201(d)(5), 116 Stat. 2135, 2146 (2002); 6 U.S.C. § 121(d)(5). DHS updated the NIPP in January 2009 to include a greater emphasis on resiliency. See DHS, *National Infrastructure Protection Plan, Partnering to Enhance Protection and Resiliency* (Washington, D.C.: Jan. 2009). DHS again updated the NIPP in December 2013 to emphasize the integration of physical and cybersecurity into the risk management framework. See DHS, *2013 National Infrastructure Protection Plan, Partnering for Critical Infrastructure Security and Resilience* (Washington, D.C.: Dec. 2013).

security; and (3) the actions selected commercial airports have taken, if any, to strengthen perimeter and access control security since 2009.

This report is a public version of a prior sensitive report that we provided to you.[8] TSA deemed some of the information in the prior report Sensitive Security Information (SSI), which must be protected from public disclosure. Therefore, this report omits sensitive information regarding TSA risk assessments, programs, and directives, as well as specific airport operations, among other things. Although the information provided in this report is more limited in scope, in that it excludes such sensitive information, it addresses the same questions as the sensitive report and the methodology used for both reports is the same.

To address these questions, we analyzed general TSA data on airport security events from the Performance and Results Information System (PARIS)—TSA's system of record for regulatory activities and security events[9]—from fiscal years 2009 (October 2008) through 2015 (September 2015).[10] We selected these timeframes to align with our 2009 report on airport perimeter and access control security and the last full fiscal year of data available at the time of our review. Because TSA changed the security event reporting categories in PARIS and their definitions in October 2012, we analyzed data from fiscal years 2009 through 2012 separately from fiscal years 2013 through 2015. We reviewed data from the reporting categories in PARIS that we determined were most likely to contain security events related to perimeter and

[8] GAO, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates*, GAO-16-318SU (Washington, D.C.: Mar. 28, 2016).

[9] TSA uses PARIS for maintaining information associated with TSA's regulatory assessments, inspections, investigations, and outreach, as well as for security events and enforcement actions across transportation modes, and for recording the details of security events involving passenger and property screening.

[10] TSA defines a "security breach" as any event involving unauthorized and uncontrolled access by an individual or prohibited item into a sterile area or secured area of an airport that is determined by TSA to present an immediate and significant risk to life, safety, or the security of the transportation network which requires emergency response by law enforcement. TSA defines a "security incident" as an event that does not meet the criteria of a breach, but is reportable to PARIS as required by TSA's operations directive and guide. For the purposes of this report, a "security event" may be either a "security breach" or a "security incident."

access control security based on TSA's definitions. However, the event data that we report may over- or under-represent the total number of events directly related to perimeter and access control security. We assessed the reliability of the event data by interviewing agency officials and testing the data for missing data and duplicates, among other things. We found the PARIS event data sufficiently reliable to provide descriptive information on the number of events potentially related to perimeter and access control security over fiscal years 2009 through 2015 and by airport category.[11] See appendix I for additional details on our analysis of the PARIS data.

To determine the extent to which TSA has assessed the components of risk—threat, vulnerability, and consequence—related to commercial airport security since 2009, we analyzed documentation for TSA's risk assessment activities, such as TSA's 2013 *Comprehensive Risk Assessment for Perimeter and Access Control Security* (Risk Assessment of Airport Security) and TSA's 2013 through 2015 *Transportation Sector Security Risk Assessments* (TSSRA).[12] Specifically for vulnerability, in addition to the TSSRAs, we reviewed TSA's use of joint vulnerability assessments (JVA) that TSA conducts with support from the FBI at certain airports that TSA identifies as high-risk based on size and other factors. We analyzed the number and location of JVAs that TSA conducted since fiscal year 2009—the last year in which we reviewed JVA data—to report on the extent to which TSA has conducted a system-wide assessment of vulnerability.[13] We also interviewed TSA officials responsible for risk management activities, including risk assessments, which included representatives from the field and TSA headquarters offices. We also interviewed officials from the FBI to discuss their role in assessing threat and vulnerability through the JVA process. We compared information collected through our review of documentation and

[11] TSA classifies the nation's approximately 440 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 largest number of passenger boardings and Category IV airports have the smallest.

[12] The TSSRA is TSA's annual report to Congress on transportation security. It assesses risk by establishing risk scores for various attack scenarios within the sector, including domestic aviation.

[13] GAO-09-399.

interviews with agency officials with recommendations on risk assessment and management practices found in DHS's NIPP as well as *Standards for Internal Control in the Federal Government* and our past reports on airport perimeter and access control security.[14]

To determine the extent to which TSA has taken actions since 2009 to oversee and facilitate airport security, we asked TSA officials to identify agency-led efforts and activities that directly or indirectly affect airport security and were initiated after 2009.[15] We interviewed TSA headquarters officials responsible for various airport security activities regarding program operations as well as TSA field, airport operator, and industry association officials, as described below, regarding select TSA airport security activities. Additionally, we assessed the extent to which TSA's 2012 *National Strategy for Perimeter and Access Control Security* (Strategy) met NIPP risk management criteria.[16] We also considered the GPRA Modernization Act of 2010 (GPRAMA) requirements and generally accepted strategic planning practices for government agencies.[17]

[14] Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience,* (2013); Department of Homeland Security, *National Infrastructure Protection Plan Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach,* (2013); GAO, *Internal Control: Standards for Internal Control in the Federal Government*, GAO/AIMD-00.21.3.1 (Washington, D.C.: Nov. 1, 1999); GAO, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, GAO-04-728 (Washington, D.C.: June 4, 2004); and GAO-09-399. GAO recently revised and reissued *Standards for Internal Control in the Federal Government*, with the new revision effective beginning with fiscal year 2016. See GAO-14-704G (Washington, D.C.: Sept. 2014).

[15] We also asked TSA officials to identify agency-led activities that directly or indirectly affect airport security, were initiated prior to 2009 and were ongoing at the time of our review.

[16] In 2012, TSA released the *National Strategy for Perimeter and Access Control Security*, which defines how TSA seeks to secure airport perimeters and control access to security-restricted areas of the nation's commercial airports.

[17] Pub. L. No. 111-352, 124 Stat. 3866 (2011). The GPRA Modernization Act of 2010 (GPRAMA) updates the Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (1993). GAO, *Agencies' Strategic Plans Under GPRA: Key Questions to Facilitate Congressional Review*, GAO/GGD-10.1.16, Version 1 (Washington, D.C.: May 1997).

To describe the actions selected commercial airports have taken, if any, to strengthen airport security since 2009, we conducted site visits at 6 commercial airports. During these visits we observed airport operations and discussed security activities with airport officials and TSA federal security directors (FSD) or their representatives.[18] In addition, we interviewed by phone airport officials and FSDs or their representatives from 5 additional airports to discuss actions taken to strengthen perimeter and access control security. We selected these 11 airports for site visits and interviews based on a variety of factors, including a range in the airport category, public interest as shown through media reports of previous events to security, unique security characteristics or challenges such as a water boundary, and new technology or initiatives implemented by airports related to perimeter and access control security. Because we did not select a generalizable sample of airports, the results of these site visits and interviews cannot be projected to all of the approximately 440 commercial airports in the United States. However, these site visits and interviews provided us with onsite TSA and airport officials' perspectives on actions taken intended to strengthen airport perimeter and access control security, including various approaches using both technology- and nontechnology-based methods. Further, we interviewed officials from two industry associations and two specialist non-profit organizations based on input from TSA officials and airport officials, and because of these associations' specialized knowledge and experience with airport security operations.[19] Additional details on our scope and methodology are contained in appendix I.

We conducted this performance audit from February 2015 to May 2016, in accordance with generally accepted government auditing standards.

[18] FSDs are the ranking TSA authorities responsible for leading and coordinating TSA security activities at the nation's approximately 440 commercial airports.

[19] According to the two industry associations—American Association of Airport Executives (AAAE) and Airports Council International-North America (ACI-NA)—their combined membership includes thousands of airport management personnel and represents approximately 95 percent of domestic airline passenger and air cargo traffic in North America. The two non-profit organizations—National Safe Skies Alliance, Inc., and RTCA, Inc., a federal aviation advisory committee formerly known as the Radio Technical Commission for Aeronautics—work with airports, government, and the industry to develop related technologies and procedures. RTCA also functions as a federal advisory committee for the review and endorsement of recommendations on a variety of issues—such as technical performance standards—for the Federal Aviation Administration (FAA).

Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

# Background

## Airport Perimeter and Access Control Security Roles and Responsibilities

TSA assumed primary responsibility for implementing and overseeing the security of the nation's civil aviation system following the terrorist attacks of September 11, 2001.[20] This includes regulating and providing guidance for airports' and air carriers' actions and performing its own actions to maintain and improve the security of their perimeters and access controls as well as establishing and implementing measures to reduce the security risks posed by aviation workers. As of March 2015, TSA had 80 FSDs who oversee the implementation of, and adherence to, TSA requirements at approximately 440 commercial airports nationwide. As the regulatory authority for civil aviation security, TSA inspects airports, air carriers, and other regulated entities to ensure they are in compliance with federal aviation security regulations, TSA-approved airport security programs, and other requirements.[21] For a list of federal requirements pertaining to perimeter and access control security, see appendix II. TSA oversees security operations at airports through compliance inspections, covert

[20] See 49 U.S.C. § 114(d).

[21] See generally 49 C.F.R. pt. 1542. Most commercial airports discussed in this report, which, in general, are those regularly serving domestic (i.e., U.S.) and foreign air carriers with scheduled passenger operations, operate under "complete" security programs that contain the most comprehensive security measures. See 49 C.F.R. § 1542.103(a). Other airports that, in general, regularly serve smaller air carrier operations, 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. In general, airport security programs may be amended, either by TSA or at the request of an airport operator. 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 (providing, among other things, that each airport operator must comply with an applicable security directive within the time prescribed by the security directive).

testing, and vulnerability assessments to analyze and improve security, among other activities.[22] In general, TSA funds its perimeter and access control security-related activities out of its annual appropriation.[23] TSA also does not generally provide funds directly to airport operators for perimeter and access control security efforts. Funding to address perimeter and access control security needs may, however, be made available to airport operators through other sources, including the Federal Aviation Administration's (FAA) Airport Improvement Program.[24]

Airport operators have direct responsibility for implementing security requirements in accordance with their TSA-approved airport security programs. Airport security programs generally cover the day-to-day aviation operations and implement security requirements for which commercial airports are responsible, including the security of perimeters and access controls protecting security-restricted areas. Among other things, these security programs include procedures for performing background checks on aviation workers and applicable training programs for these workers. Further, airport security programs must also include descriptions of the security-restricted areas—that is, areas of the airport identified in their respective security programs for which access is

[22] For example, pursuant to ATSA, TSA must on an ongoing basis, assess and test for compliance with access control requirements, report annually on the findings of the assessments, assess the effectiveness of penalties in ensuring compliance with security procedures, and take any other appropriate enforcement actions when noncompliance is found. See 49 U.S.C. § 44903(g)(2)(D). 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.

[23] GAO-09-399. Examples of TSA's perimeter and access control security activities include, among other things, airport compliance inspections, JVAs, Playbook aviation worker screening operations, and Visible Intermodal Prevention and Response (VIPR) teams. VIPR teams, which include TSA and law enforcement personnel, perform various functions that include randomly inspecting workers, property, and vehicles, as well as patrolling all modes of transportation, including the aviation sector.

[24] Through the FAA-administered Airport Improvement Program, grants are available to public agencies and, in some cases, to private owners and entities, for the planning and development of public-use airports that have been designated as significant to national air transportation. Airport Improvement Program funding is also available to airport operators for limited security-related purposes. According to TSA officials, TSA monitors $5 million of this funding awarded annually by the FAA to the National Safe Skies Alliance, Inc.

controlled and the general public is generally not permitted entry—including a map detailing boundaries and pertinent features of the security-restricted areas.[25] Although, pursuant to regulatory requirements, the components of airport security programs are generally consistent across airports, the details of these programs and their implementation can differ widely based on the individual characteristics of airports.

TSA generally characterizes airport perimeter security at commercial airports to include protection of the fence line—or perimeter barriers—vehicle and pedestrian gates, maintenance and construction gates, and vehicle roadways, as well as general aviation areas.[26] Access control security generally refers to security features that control access to security-restricted areas of the airport that may include baggage makeup areas, catering facilities, cargo facilities, and fuel farms. Specifically, airport perimeter and access control security measures are designed to prevent unauthorized access onto the airport complex and into security-restricted areas. For example, airport operators determine the boundaries for the security-restricted areas of their airport based on the physical layout of the airport and in accordance with TSA requirements. Security programs for commercial airports generally identify designated areas that

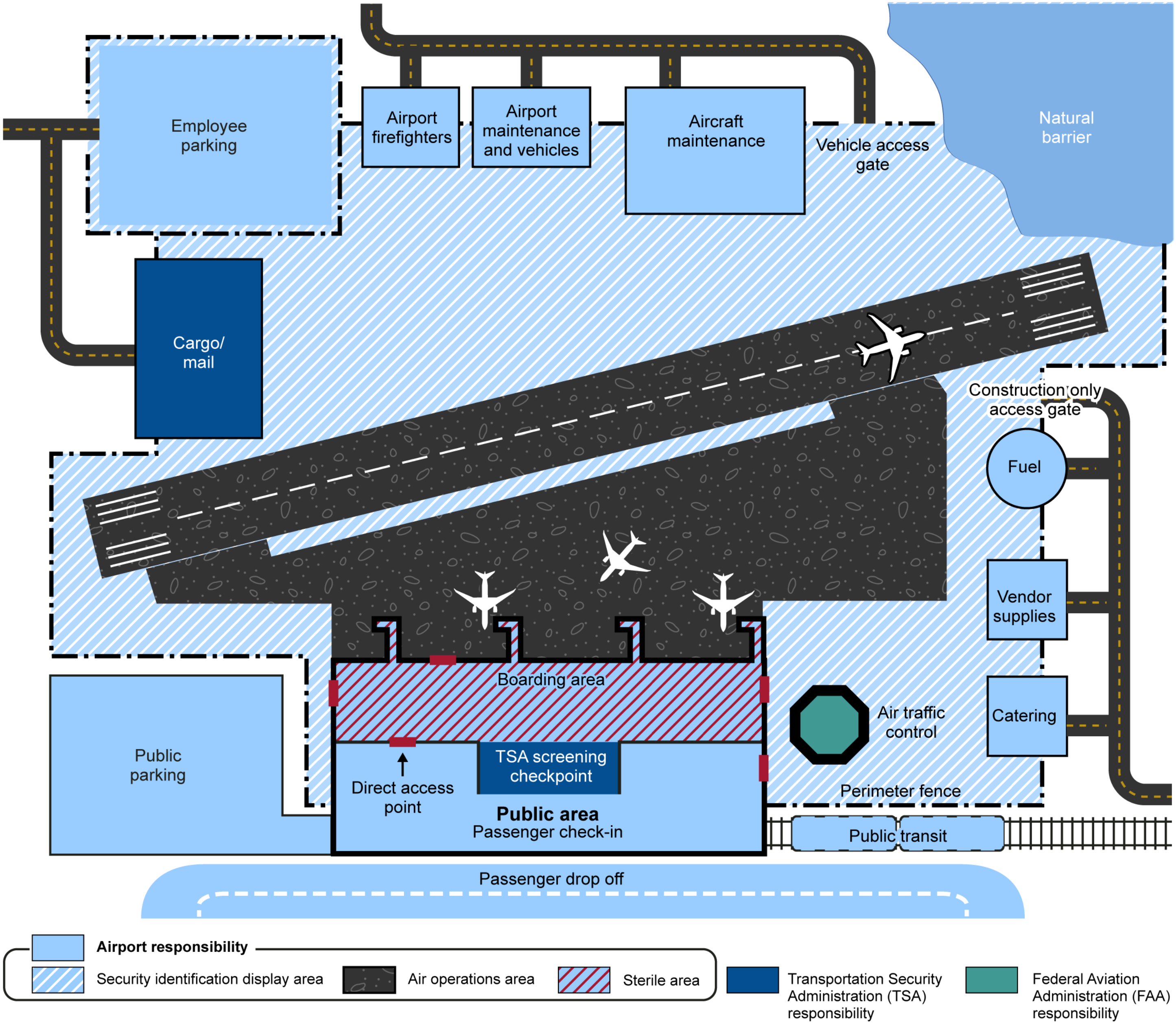
[25] See 49 C.F.R. § 1542.103(a)(3)-(6). For the purposes of this report "security-restricted area" is used generally to refer to areas specified in an airport security program that require restricted access, including the secured area, security identification display area (SIDA), Air Operations Area (AOA), and sterile area. While security measures governing access to such areas may vary, in general a "secured area" is where aircraft operators with security programs enplane and deplane passengers and sort and load baggage and any adjacent areas that are not separated by adequate security measures, a SIDA is an area in which appropriate identification must be worn, and an AOA is an area providing access to aircraft movement and parking areas. See 49 C.F.R. § 1540.5. The sterile area is the area of an airport that provides passengers access to boarding aircraft and is an area to which access is generally controlled by TSA or a private screening entity under TSA oversight. See *id.*

[26] "General aviation" refers to all civil aviation except scheduled passenger and cargo operations and excludes military flights. General aviation traffic ranges from small propeller planes flying from private runways to large jets based at major airports. A general aviation airport is any area of land or water used or intended for use by an aircraft to land or take off, including any buildings or facilities therein, but generally does not include airports subject to security requirements under 49 C.F.R. part 1542, such as airports with scheduled passenger (i.e., commercial) operations. Some airports support both scheduled commercial and general aviation operations. General aviation operations range from small propeller planes flying from private runways to large jets based at major airports.

have varying levels of security, known as secured areas, security identification display area (SIDA), Air Operations Area (AOA), and sterile areas (referred to collectively in this report as “security-restricted areas”). For example, passengers are not permitted unescorted access to secured areas, SIDAs, or the AOA, which typically encompass baggage loading areas, areas near terminal buildings, and other areas close to parked aircraft and airport facilities, as illustrated in figure 1. Aviation workers may access the sterile area through the security checkpoint (at which time they undergo screening similar but not identical to that experienced by a passenger) or through other access points secured by the airport operator in accordance with its security program.[27]

[27] In general, certain aviation workers and other credentialed personnel at airports, such as personnel with valid SIDA credentials, uniformed flight crewmembers, or properly credentialed FAA safety inspectors—who enter the sterile area through the passenger screening checkpoint for the purpose of performing work-related duties— may undergo expedited screening, which permits them to pass through the checkpoint without, for example, removing footwear or light outer garments (such as suit jackets). For more information on expedited screening, see GAO, *Aviation Security: Rapid Growth in Expedited Passenger Screening Highlights Need to Plan Effective Security Assessments*, GAO-15-150 (Washington, D.C.: Dec. 12, 2014). Aviation workers with a need for an item that is otherwise prohibited in the sterile area or onboard an aircraft for the performance of their duties may use and be in possession of such items in the sterile area but may not take these items through the screening checkpoints. Additionally, airport and aircraft operators must notify aviation workers traveling as passengers that they must access the sterile area through the TSA screening checkpoint with any accessible property they intend to carry onboard the aircraft and remain in the sterile area after entering.

Figure 1: Security-Restricted Areas of a Commercial Airport in the United States



Source: GAO. | GAO-16-632

Note: This figure shows airport security-restricted areas designated in accordance with TSA requirements. Pursuant to 49 C.F.R. § 1542.205, each airport area defined as a secured area in a security program must be a SIDA, though other areas of the airport may also be designated as SIDAs by the airport operator. For example, some airport operators designate all AOAs as SIDAs.

Airport operators are responsible for safeguarding their perimeter barriers, preventing and detecting unauthorized entry, and conducting background checks of workers with unescorted access to secured areas. Methods used by airports to control access through perimeters or into security-restricted areas vary because of differences in the design and layout of individual airports, but all access controls must meet minimum performance standards in accordance with TSA requirements. These methods typically involve the use of one or more of the following: pedestrian and vehicle gates; keypad access codes using personal identification numbers, magnetic stripe cards and readers; biometric (e.g., fingerprint) readers; turnstiles; locks and keys; and security personnel (e.g., guards).

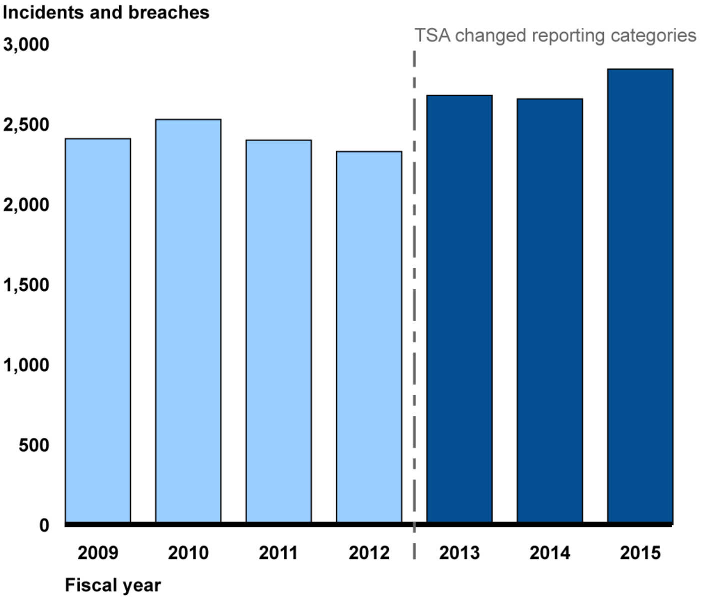
TSA requires FSDs or their designees to report security events that occur both at the airports for which they are responsible and on board aircraft destined for their airports. TSA collects airport security event data from airports and stores that information in numerous systems.[28] In addition to PARIS, TSA uses the Security Incident Reporting Tool (SIRT)—a tool designed for root cause analysis, among other things—to record security event information in the field (e.g., at airports).[29] Events that TSA reports to these systems may include a range of occurrences, such as an inebriated driver crashing through a perimeter fence or a baggage handler using his access to smuggle drugs to outbound passengers.

In October 2012, TSA updated its operations directive related to reporting security events. While TSA redefined some event categories and expanded the overall number of event categories, these event categories are not specific for events that relate to perimeter or access control. As a result, the number of events that directly relate to perimeter and access control security may be over- or under-represented in any analysis. Figure 2 shows the estimated number of events potentially related to perimeter and access control security from fiscal years 2009 through 2015, by fiscal year.

[28] TSA also uses the Airport Information Management (AIM) system, Transportation Information Sharing System, and Web Emergency Operations Center system for other purposes related to management of aviation security.

[29] According to TSA officials, SIRT includes much of the same information found in PARIS security event records but in a format that more easily allows performance analysis and reporting, root cause analysis, and corrective action tracking.

Figure 2: Select Events Potentially Related to Airport Perimeter and Access Control Security Reported in Transportation Security Administration's (TSA) Performance and Results Information System (PARIS)



Source: GAO analysis of TSA PARIS data. | GAO-16-632

Note: We selected categories that were most likely to contain events related to perimeter and access control security for fiscal years 2009 through 2012, which included "access control," "perimeter breach," "perimeter event," and "security breach." We also selected categories that were most likely to contain events related to perimeter and access control security for fiscal years 2013 through 2015, which include "access control – contained," "access control – delayed," "security breach," and "stowaway." We identified these event categories in PARIS as those that were most likely to include perimeter and access control security events. We further refined the data by removing those events that TSA identified as having occurred at an operational passenger screening checkpoint, which is specifically excluded from TSA's definition of perimeter and access control security. However, these categories include events that are not directly related to perimeter and access control security, and other event categories in PARIS may include events that are related. See appendix I for additional details on our analysis of PARIS event data.

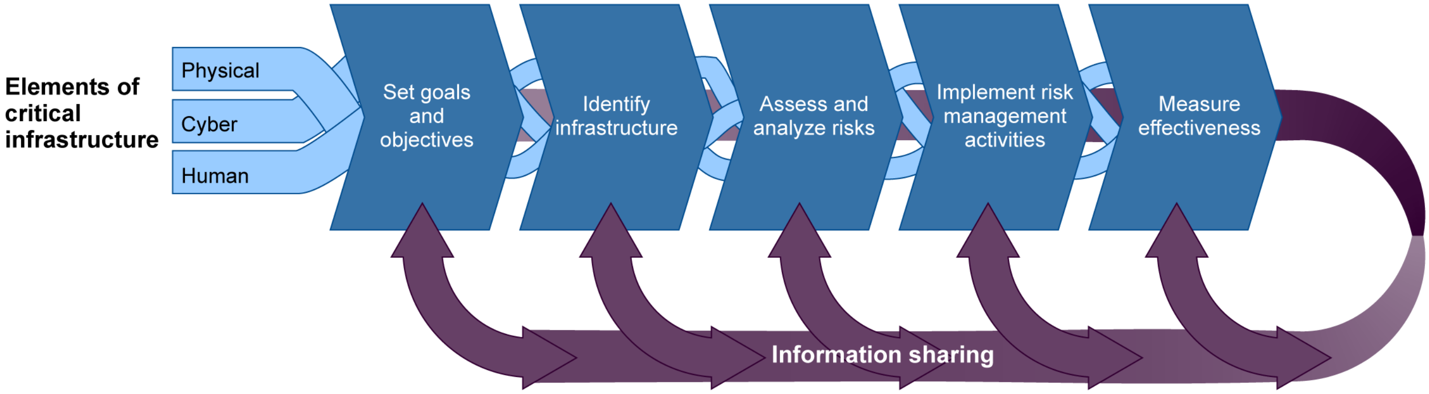
## Risk Management Approach

Since it is not feasible to protect all assets and systems against every possible threat, DHS uses a risk management approach to prioritize its investments, develop plans, and allocate resources in a risk-informed way that balances security and commerce.[30] Risk management calls for a cost-effective use of resources and focuses on developing and implementing protective actions that offer the greatest mitigation of risk for any given expenditure. A risk management approach entails a continual process of managing risk through a series of actions, including setting goals and objectives, assessing risk, evaluating alternatives, selecting initiatives to undertake, and implementing and monitoring those initiatives. DHS developed the NIPP, which establishes a risk management framework to help its critical infrastructure stakeholders determine where and how to invest limited resources. In accordance with the Homeland Security Act of 2002 and Homeland Security Presidential Directive/HSPD-7, DHS released the NIPP in 2006, which it later updated in 2009 and 2013.[31] The NIPP risk management framework includes setting goals and objectives, identifying infrastructure, assessing and analyzing risks, implementing risk management activities, and measuring effectiveness. This framework constitutes a continuous process that is informed by information sharing among critical infrastructure partners. See figure 3 for these elements of critical infrastructure risk management.

[30] In the context of risk management, “risk-based” and “risk-informed” are often used interchangeably to describe the related decision-making processes. However, according to the DHS Risk Lexicon, risk-based decision making uses the assessment of risk as the primary decision driver, while risk-informed decision making may consider other relevant factors in addition to risk assessment information. Because it is an acceptable DHS practice to use other information in addition to risk assessment information to inform decisions, we have used “risk-informed” throughout this report.

[31] See 6 U .S.C. § 121(d)(5); Homeland Security Presidential Directive/HSPD-7 (Dec. 17, 2003). See also Presidential Policy Directive/PPD-21 (Feb. 12, 2013) (revoking HSPD-7 but providing that plans developed pursuant to HSPD-7 shall remain in effect until specifically revoked or superseded).

Figure 3: National Infrastructure Protection Plan (NIPP) Critical Infrastructure Risk Management Framework



Source: GAO presentation of NIPP framework. | GAO-16-632

The NIPP sets forth risk management principles that include a comprehensive risk assessment process that requires agencies to consider all elements of risk—threat, vulnerability, and consequence. These elements are defined as the following:

- Threat is a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. For the purpose of calculating risk, the threat of an intentional hazard is generally estimated as the likelihood of an attack being attempted by an adversary. The threat likelihood is estimated based on the intent and capability of the adversary.
- Vulnerability is a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. In calculating the risk of an intentional threat, a common measure of vulnerability is the likelihood that an attack is successful, given that it is attempted.
- Consequence is the negative effect of an event, incident, or occurrence.

## TSA Has Made Progress Assessing Risks to Airport Security, but Limitations Remain in Updating Assessments, Assessing System-wide Vulnerability, and Monitoring Trends

### TSA Has Assessed All Three Components of Risk

Since 2009, TSA has made progress in assessing all three components of risk—threat, vulnerability, and consequence—partly in response to our 2009 recommendations.[32] Specifically, in May 2013, TSA developed its *Comprehensive Risk Assessment of Perimeter and Access Control Security* (Risk Assessment of Airport Security). This assessment was based primarily on information from other TSA efforts to assess airport security risks or components of risk, such as the TSSRA TSA issued in 2013, JVAs TSA conducted with the FBI at select airports in fiscal year 2011, and a Special Emphasis Assessment conducted in September 2012. The TSSRA, TSA's annual report to Congress on transportation security, establishes risk scores and assesses threat, vulnerability, and consequence for various attack scenarios to all modes within the transportation sector, including domestic aviation.[33] TSA's Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) conducts JVAs every 3 years at commercial airports in the United States identified as high risk (referred to as "triennial" airports) and on a case-by-case basis

[32] See GAO-09-399.

[33] For example, one of the TSSRA attack scenarios related to airport perimeter and access control security is an attack on an aircraft on the ground at an airport.

for other commercial airports.[34] TSA's Office of Security Operations led the Special Emphasis Assessment—a national assessment of a particular aviation security area of emphasis—specifically for the Risk Assessment of Airport Security.[35] For each component of risk, TSA has taken the following broad assessment actions that include actions related to airport perimeter and access control security:

- **Threat.** TSA has assessed threats of various attack scenarios for domestic aviation through the TSSRAs, the latest version of which TSA released to Congress in July 2015. In this version of the TSSRA, TSA identified numerous attack scenarios related to domestic aviation, including airport security. These scenarios include threat scores, which TSA estimated on the basis of intent and capability of al-Qaeda, its affiliates, and its adherents as the expected adversary.[36] In addition, as part of the JVA process, the FBI produces a threat intelligence report. According to FBI officials, they provide this report to the airports' FSDs and make the reports available to the JVA teams prior to the scheduled JVA.[37]
- **Vulnerability.** TSA officials stated that their primary measures for assessing the vulnerability of commercial airports to attack—including

[34] See 49 U.S.C. § 44904; Pub. L. No. 104-264, § 310, 110 Stat. 3213, 3253 (1996). According to TSA officials, a JVA is not intended to be a review of an airport's compliance with security requirements, and TSA does not impose penalties for any instances of noncompliance discovered through a JVA. JVA teams assess all aspects of airport security and operations, beyond perimeter security and access controls, to include fuel, cargo, catering, general aviation, terminal area, and law enforcement operations.

[35] According to TSA officials, Special Emphasis Assessments are typically short-term, lasting a few weeks to a few months. TSA uses Special Emphasis Assessments to assess vulnerabilities in a targeted area of emphasis where there may not be specific regulatory requirements. Thus, TSA does not typically use Special Emphasis Assessments to levy enforcement action against an airport operator or other regulated entity.

[36] TSA previously reported on threats on an annual basis in the Civil Aviation Threat Assessment (CATA), which established an annual baseline assessment of threat to U.S. aviation by reviewing terrorist threats to U.S. civil aviation worldwide. TSA's most recent CATA was dated November 2012. TSA officials stated that as of February 2015 they were reconfiguring CATA with the assistance of contractors. TSA officials were unsure as to when the reconfigured CATA would be finalized.

[37] As part of the FBI's Civil Aviation Security Program and to mitigate threats to aviation, the FBI also produces and distributes daily aviation-centric intelligence summaries to aviation liaison agents assigned to the nation's commercial airports.

assessing security of perimeter and access controls—is the JVA process and professional judgment. TSA has increased the number of JVAs conducted at commercial airports since 2009. In 2009, we reported that TSA conducted JVAs at 57 (13 percent) of the nation's then approximately 450 commercial airports since fiscal year 2004.[38] As of the end of fiscal year 2015, TSA conducted JVAs at 81 (about 19 percent) of the 437 airports since fiscal year 2009.[39] In addition, TSA has also assessed the vulnerability of airports through the TSSRAs by assigning numerical values to the vulnerability of each attack scenario and related countermeasures based on the judgements of TSA and other subject matter experts, such as airport officials.

- **Consequence.** TSA has assessed consequence through the TSSRAs by analyzing both direct and indirect consequences of the various attack scenarios related to domestic airports. According to the TSSRAs, direct consequences (or impacts) include the immediate economic damage following an attack that includes infrastructure replacement costs, deaths, and injuries. Indirect consequences are the secondary macro- and micro-economic impacts that may include the subsequent impact on supply chains, loss of revenues, consumer behaviors, and other downstream costs.

To further address components of risk, TSA established an integrated project team in the summer of 2015 to plan for the development of a compliance-based risk assessment. The intent of this effort, according to TSA officials, is to leverage compliance inspections findings as well as other assessment data to yield a risk level that incorporates threat, vulnerability, and consequence for all regulated airports and other entities. TSA officials stated that this new planned effort will differ from the Risk Assessment of Airport Security in that they intend it to be an ongoing process that will be more operational in nature. TSA officials stated that this effort is in its infancy, and will not be developed and implemented until at least fiscal year 2018.

[38] In GAO-09-399, we stated that there were approximately 450 TSA-regulated (i.e., commercial) airports in the United States, and all calculations we reported in 2009 were based on the 450-airport count. However, as of September 2015, there were 437 commercial airports, and all new calculations are based on this number.

[39] From fiscal years 2004 through 2015, TSA conducted JVAs at 98 of the 437 commercial airports.

## TSA Has Not Updated Its Risk Assessment of Airport Perimeter and Access Control Security or Shared Updated Risk Information with Stakeholders

While TSA released its Risk Assessment of Airport Security in May 2013, it has not updated this assessment to reflect changes in the airport security risk environment or routinely shared updated national risk information with airports or other stakeholders. Specifically, TSA based its Risk Assessment of Airport Security primarily on information from the TSSRA submitted to Congress in May 2013, JVAs conducted in fiscal year 2011, and a Special Emphasis Assessment conducted in September 2012. However, since completion of its Risk Assessment of Airport Security in 2013, TSA has not updated it with information TSA submitted to Congress in the July 2014 and July 2015 versions of the TSSRA. TSA updated these versions of the TSSRA to include additional attack scenarios related to domestic aviation and to reflect an increase in threat scores across all modes of transportation. In the July 2015 TSSRA, TSA stated that one scenario would relate directly to airport security.[40] Furthermore, TSA expanded the 2014 and 2015 TSSRA versions to assess risk from the insider threat.[41] In the latest TSSRA assessment of insider threat, TSA stated that although all domestic aviation-specific scenarios (presented in the July 2014 TSSRA) could be executed without insider support, approximately 65 percent of the attack scenarios would be more easily facilitated by a TSA insider. In this version of the TSSRA, TSA also reported that it should extend the concept of insider threat beyond the TSA workforce to all individuals with privileged access—e.g., aviation workers. TSA also conducted 72 JVAs in fiscal years 2012 through 2015, the results of which are not reflected in TSA's May 2013 Risk Assessment of Airport Security. Further, TSA's 2013 assessment relied upon results from a Special Emphasis Assessment that was specifically conducted over a 2-week period in September 2012 to gather physical security data for the Risk Assessment of Perimeter Security from Category X, I, II, and III airports (approximately 67 percent of the about 440 commercial airports and accounting for all airports required by TSA to have a complete security program).

[40] TSA determined the specific details of this attack scenario to be Sensitive Security Information (SSI). Therefore, we do not discuss the details of the scenario.

[41] The TSSRAs define insiders related to domestic commercial aviation as one or more individuals with access or knowledge that allows them to exploit vulnerabilities in the nation's aviation sector with intent to cause harm. These individuals are, or present themselves to be, current or former aviation employees, contractors, or partners who have or have had authorized access to aviation sector facilities, operations, systems, and information.

As part of the Risk Assessment of Airport Security, TSA discussed ongoing actions to share summary information from this assessment with airport FSDs through email and with airport operators on its external website's communications board. This summary included high-level information related to perimeter and access control security that was based on the 2013 version of the TSSRA, 24 JVAs TSA conducted in fiscal year 2011 at select airports, and the Special Emphasis Assessment that TSA conducted at selected airports in September 2012. For example, TSA shared the perimeter components that had the highest number of JVA findings and the Special Emphasis Assessment's topics of concern.[42] According to TSA officials, TSA has not continued to share updated summary information in this format from the JVAs conducted since fiscal year 2011 or from the additional Special Emphasis Assessment related to perimeter and access control security that TSA conducted in November 2012 with airport operators on a broad scale.[43]

The NIPP states that effective risk management calls for updating assessments of risk and its components as pertinent information becomes available. The NIPP also states that agencies should share actionable and relevant information across the critical infrastructure community—including airport operators—to build awareness and enable risk-informed decision-making as these stakeholders are crucial consumers of risk information. Further, *Standards for Internal Control in the Federal Government* states that agencies should identify, analyze, and respond to changes and related risks that may impact internal control systems as part of its risk assessment process, and agencies should communicate with external parties so that these parties may help the agency achieve its objectives and address related risks.[44]

[42] TSA determined the perimeter components that had the highest number of JVA findings and the Special Emphasis Assessment's topics of concern to be SSI. Therefore, we do not identify those components and topics.

[43] TSA officials stated that they have shared airport security-related results from the agency's Compliance Security Enhancement Through Testing (COMSETT) with industry associations, individual airports, and airlines. COMSETT is an airport and airline compliance testing procedure that uses a three-phased approach to compliance testing. According to TSA officials, absent significant egregious or aggravating circumstances, penalties for failed tests are not imposed until airports have been given an opportunity to address compliance issues.

[44] See GAO/AIMD-00-21.3.1.

TSA officials have acknowledged that they have not updated the Risk Assessment of Airport Security and do not have plans or a process to update it, or share updated summary information, such as information from JVAs and Special Emphasis Assessments, with airport operators on an ongoing basis. TSA officials agreed that updating the JVA summary information to share with airport operators and other stakeholders, for example, could be useful. However, TSA officials also stated that TSA does not have an effective JVA information collection tool that allows systematic analysis that could enable TSA to share summary information readily with airport operators on an ongoing, continuous basis. Further, TSA officials said they do not have a process for determining when additional updates to the Risk Assessment of Airport Security are needed or when the updated information should be shared. TSA's Chief Risk Officer stated that TSA currently determines when and how to update its assessments based on judgment and that TSA should update its Risk Assessment of Airport Security to reflect new information regarding the risk environment. The Chief Risk Officer agreed that TSA's oversight of airport security could benefit from updating and sharing the Risk Assessment of Airport Security on an ongoing basis as well as establishing a process for determining when additional updates are needed.

TSA officials stated that they perceive the Risk Assessment of Airport Security as its primary mechanism for cohesively addressing perimeter and access control security risk issues and sharing that summary information with stakeholders. Further given the changes in the risk environment reflected in the latest versions of TSSRA, including the insider threat, and the additional JVAs and the Special Emphasis Assessment, TSA's Risk Assessment of Airport Security is not up-to-date. According to both TSA and the FBI, the insider threat is one of aviation security's most pressing concerns. Insiders have significant advantages over others who intend harm to an organization because insiders may have awareness of their organization's vulnerabilities, such as loosely enforced policies and procedures, or exploitable security measures. The July 2015 TSSRA states that approximately 65 percent of the domestic aviation-specific attack scenarios would be more easily facilitated by a TSA insider. As such, updating the Risk Assessment of Airport Security with TSSRA information that reflects this current, pressing threat as well as with findings from JVAs already conducted, future Special Emphasis Assessments, and any other TSA risk assessment activities would better ensure TSA is basing its risk management decisions on current information and focusing its limited resources on the highest-priority risks to airport security. Sharing information from the updated Risk Assessment of Airport Security with airport security stakeholders on an ongoing basis, including any broader findings from JVAs or Special Emphasis Assessments conducted to date, may enrich airport operators' understanding of and ability to reduce vulnerabilities identified at their airports. Furthermore, establishing a process for determining when additional updates to the Risk Assessment of Airport Security are needed would ensure that future changes in the risk environment are reflected in TSA's mechanism for culminating and sharing risk information related to perimeter and access control security.

## TSA Has Not Assessed Vulnerability of Airports System-wide

TSA has not comprehensively assessed the vulnerability of airports system-wide through its JVA process—its primary measure for assessing vulnerability at commercial airports. In 2009, we recommended that TSA develop a comprehensive risk assessment for airport perimeter and access control security. As part of that effort, we recommended that TSA should evaluate whether its then current approach to conducting JVAs reasonably assessed vulnerabilities at airports system-wide, and whether an assessment of security vulnerabilities at airports nationwide should be conducted. TSA officials stated in response to our recommendation that its approach to conducting JVAs appropriately assessed vulnerabilities, but a future nationwide assessment of all airports' vulnerability would be appropriate to improve security. Since our 2009 report, TSA conducted JVAs at 81 commercial airports (approximately 19 percent of the roughly 440 commercial airports nationwide) from fiscal years 2009 through 2015; however, the majority of these airports were either Category X or I airports. TSA officials stated that TSA primarily limits the JVAs it conducts on a routine, triennial basis to 34 Category X through II airports that the Federal Aviation Administration (FAA) determined to be high risk based on a variety of factors.[45] In addition to the triennial airports, TSA has selected other airports for JVAs at the direction of DHS or TSA senior

[45] According to TSA officials, prior to the formation of DHS and TSA's taking responsibility for JVAs, FAA identified these 34 airports as high risk based on a variety of factors such as size of aircraft services, number of enplanements, category of airport, last point of departure, and air cargo volume, among other things. TSA officials stated that they have continued to use these originally-selected 34 airports as the airports that are required to have a JVA on a triennial basis.

leadership or at the request of the FBI.[46] See table 1 for the number and percent of JVAs conducted by airport category.

**Table 1: The Number of Joint Vulnerability Assessments (JVA) Conducted by Airport Category, from Fiscal Years 2009 through 2015**

| Airport category | Number of JVAs conducted | Number of commercial airports by category | Percent of category |
|---|---:|---:|---:|
| Category X | 28 | 28 | 100 percent |
| Category I | 33 | 57 | 58 percent |
| Category II | 15 | 82 | 18 percent |
| Category III | 5 | 125 | 4 percent |
| Category IV | 0 | 145 | 0 percent |
| **All categories** | **81** | **437** | **19 percent** |

Source: GAO analysis of TSA data. I GAO-16-632

Note: We reported the JVAs by commercial airport category as categorized in September 2015. The categories of some airports may have changed from the time of the JVA to our analysis. None of the airports that received a JVA dropped off the list of TSA-regulated (i.e., commercial) airports as of September 2015. Percentages are rounded.

TSA does not include Category III and IV airports in the triennial JVA process. Further, TSA has conducted 5 JVAs at Category III airports and has not conducted any JVAs at Category IV airports, both of which make up approximately 62 percent of commercial airports system-wide. Our analysis of PARIS event data shows that these airports have experienced security events potentially related to perimeter and access control security, which may demonstrate vulnerabilities to airport security applicable across smaller airports system-wide. We found that over 1,670 events, or approximately 9.4 percent of total events that we analyzed over the time period, occurred at Category III and IV airports since fiscal year 2009.[47] These events included, for example, individuals driving cars through or climbing airports' perimeter fences and aviation workers

[46] TSA and FBI officials stated that TSA is responsible for choosing which airports outside of those triennial airports are to receive JVAs and determining the total number of JVAs conducted. Further, TSA typically conducts the assessment at the airport while the FBI provides support before the JVA through the threat intelligence report and following the JVA during a joint TSA and FBI briefing with airport officials.

[47] These events included the security event reporting categories in PARIS that we included in our analysis of events that potentially related to perimeter and access control security.

allowing others to follow them through airport access portals against protocol.

The NIPP requires a system-wide—or nationwide—assessment of vulnerability to inform a comprehensive risk assessment and an agency's risk management approach. The NIPP supplement states that risk assessments may explicitly consider vulnerability in a quantitative or qualitative manner, and must consider and address any interdependencies between how the vulnerabilities and threats were calculated. Also, the vulnerability assessment may be a standalone product or part of a full risk assessment and is to involve the evaluation of specific threats to the asset, system, or network in order to identify areas of weakness that could result in consequences of concern. In our 2004 and 2009 reports, TSA officials told us that a future nationwide vulnerability assessment would improve overall domestic aviation security.[48] While TSA has since expanded the number of airports at which it has conducted JVAs (increasing from 13 percent through fiscal year 2008 to about 19 percent through fiscal year 2015), TSA officials stated that they have not conducted analyses to determine whether the JVAs are reasonably representative to allow for some system-wide judgment of commercial airports' vulnerability. Therefore, they cannot ensure that the JVAs represent a system-wide assessment and provide a complete picture of vulnerabilities at all airports, including for those airports categorized as III or IV.

TSA officials stated that they are limited in the number of JVAs they conduct because of resource constraints. Specifically, officials stated that JVAs are resource intensive—typically requiring 30 days of advance preparation, about one week for a team of 2 to 5 staff to conduct the JVA, and 60 days to finalize the written report. Further, TSA officials stated that they have limited resources to conduct JVAs above and beyond the 34 triennial airports. As a result, TSA officials said the agency has conducted JVAs at 4 to 6 additional airports per year beyond the triennial airports they identified as high risk and, therefore, have not been able to conduct JVAs at all airports system-wide.[49] FBI officials stated that they defer to

[48] See GAO-04-728 and GAO-09-399.

[49] TSA officials said they conduct JVAs at these additional areas for a variety of reasons such as a scheduled National Security Special Event nearby or other big event such as the Super Bowl.

TSA on whether to increase the number of JVAs, and have previously been able to manage increases in the number conducted without a significant strain on FBI's resources. In 2010, TSA developed an airport self-vulnerability assessment tool; however, TSA's policy is to provide the tool to airports already selected for a JVA in order to inform their assessment, and has not provided it to all airports as a means to inform TSA's selection of airports for JVAs or to assess vulnerability in lieu of a JVA. Further, in 2011, TSA developed and deployed the Airport Security Self-Evaluation Tool (ASSET) to provide airports with a tool to evaluate their current level of security and compare their activities to specific security measures identified by TSA. However, TSA officials stated that while ASSET was made available to airports on TSA's external website's communication board, the tool did not have widespread acceptance or use, possibly due to its technical nature since it requires use of specific software. TSA has subsequently stopped pursuing its industry-wide use. In addition to the JVAs and self-assessment tools, TSA officials stated that their regulatory compliance inspections that TSA inspectors conduct at airports at least annually augment their vulnerability assessments at individual airports. However, compliance inspections of an individual airport's adherence to federal regulations, while helpful in potentially identifying those airports that would benefit from further vulnerability assessment, do not constitute a system-wide vulnerability assessment. Furthermore, TSA did not include the results of compliance inspections in the Risk Assessment of Airport Security or in the JVA reports.[50]

By assessing vulnerability of airports system-wide, TSA could better ensure that it has comprehensively assessed risks to commercial airports' perimeter and access control security. The events that occurred at Category III and IV airports may not have garnered the same media attention, or produced the same consequences, as those at larger airports. However, they are part of what TSA characterizes as a system of interdependent airport hubs and spokes in which the security of all is affected by the security of the weakest one. Consequently, TSA officials

[50] While airports' or air carriers' compliance with regulations suggests less vulnerability, the intent of TSA's compliance inspections differs from that of a JVA or other forms of broader vulnerability assessment in that compliance inspections assess regulated entities' meeting the baseline requirements while JVAs assess vulnerability above and beyond the requirements. According to TSA officials, TSA inspectors are authorized to look for and address with airport operators issues that go beyond the baseline requirements.

stated that the interdependent nature of the system necessitates that TSA protect the overall system as well as individual assets or airports. While we recognize that conducting JVAs at all or a statistically representative sample of the approximately 440 commercial airports in the United States may not be feasible given budget and resource constraints, other approaches to assessing vulnerability may allow TSA to assess vulnerability at airports system-wide. For example, outside of the 34 triennial airports, TSA could select a sample that would reflect a broader representation of airports, including Category III and IV airports, or TSA could provide airports with self-vulnerability assessment tools, the results of which TSA could collect and analyze to inform its understanding of system-wide vulnerabilities.

## TSA Does Not Analyze Its Security Event Data Specifically for Perimeter and Access Control Security

TSA does not analyze its security event data to monitor security events at airports for those specifically related to perimeter and access control security. TSA officials stated that PARIS—TSA's system of record for security events—is a data repository, among other things. As such, TSA officials stated they cannot easily analyze PARIS data without broadly searching for events potentially related to perimeter and access control and then further analyzing the content of the narratives that make up the majority of the information provided in PARIS. According to officials, this type of query and content analysis of PARIS data would be a laborious and time-consuming process because the events and the associated descriptive narratives are unique, and searching for common terminology that would ensure all relevant events were captured would be challenging. For example, a search of "insider" or "employee" would not necessarily return all events that involved an insider. Because of the mostly narrative content, TSA is unable to readily identify and analyze those entries directly related to airport perimeter and access control security within PARIS.[51]

TSA officials stated that SIRT—another TSA data system in which security event information is reported—has more built-in analytical capability and could be used for broad analysis of events related to perimeter and access control security. In a 2012 review of selected

[51] PARIS also contains structured data fields that TSA can filter using ad-hoc reporting capabilities.

airports' reporting of and TSA's response to security events, DHS's Office of Inspector General (OIG) recommended that TSA use one comprehensive definition for what constitutes a security breach and develop a comprehensive oversight program to ensure security events are accurately reported and are properly tracked and analyzed for trends.[52] In 2012, in response to the OIG's recommendations, TSA updated its operations directive for reporting security events and developed SIRT as a temporary additional tool for, among other things, analyzing the root causes of an event.[53] SIRT has built-in capabilities for performance analysis and reporting as well as root cause analysis, and the tool uses the same security event reporting categories and much of the same information as PARIS. TSA officials stated that SIRT has the capability to provide analysis of trends in perimeter and access control security events using more sophisticated built-in search tools. However, while TSA has the capability within SIRT to analyze events and TSA weekly SIRT reports include airport perimeter and access control security events as well as checkpoint events, TSA officials stated that TSA has not seen the need to regularly analyze these data for trends—including changes in trends—specifically in perimeter and access control events as TSA does in weekly reports with other security events, such as confiscation of prohibited items at checkpoints.

*Standards for Internal Control in the Federal Government* states that an agency should design its information systems to respond to the entity's objectives and risks.[54] Agencies should design a process that uses these objectives and risks to identify information requirements that consider both internal and external users. Quality information should be appropriate, current, complete, accurate, accessible, and timely. Agency management may use this information to make informed decisions and evaluate the agency's performance in achieving key objectives and addressing risks.

[52] Department of Homeland Security, Office of Inspector General, *Transportation Security Administration's Efforts to Identify and Track Security Breaches at Our Nation's Airports*, OIG-12-80 (May 2012).

[53] TSA officials stated that they developed SIRT as a temporary tool to address the OIG's recommendations until the same capability could be built into an existing platform.

[54] GAO/AIMD-00-21.3.1.

TSA officials stated that PARIS was designed to be a case management system for events that resulted in regulatory violations, and was not set up to allow for detailed analysis of all types of airport security events within the system. Although TSA revised its incident reporting operations directive in 2012 to include new event categories and developed SIRT as an enhanced analytical tool to address the OIG's findings, TSA collects much of the same information by requiring field officials to enter the same security event information in both PARIS and SIRT. As of December 2015, TSA officials stated that they are in the process of incorporating SIRT into the Airport Information Management (AIM)—a system that assists airports (and other transportation facilities) in managing day-to-day activities and includes a variety of employee and equipment information. TSA officials stated that using AIM for a single point-of-entry for security event data would be the preferred approach over duplicate data entry into SIRT and PARIS. However, TSA officials stated that the integration of SIRT into AIM is in its early stages and would occur sometime in 2016, and are unsure as to whether AIM will be the single point-of-entry for security event data. Therefore, it is unclear whether TSA's future transition of SIRT into AIM would reduce the overlapping efforts of TSA field officials by providing a single point-of-entry.

Regardless of how TSA collects security event data, using these data for specific analysis of system-wide trends related to perimeter and access control security, such as by expanding existing weekly reports to focus on perimeter and access control security events, TSA would be better positioned to use any results to inform its management of risk and assessments of risk's components.

## TSA Has Taken Actions to Oversee and Facilitate Airport Security, but Has Not Updated its Strategy to Reflect Changes in Risk Assessments and Other Actions

### TSA Has Taken Various Actions since 2009 to Oversee and Facilitate Perimeter and Access Control Security

TSA has implemented a variety of actions since 2009 to oversee and facilitate perimeter and access control security at the nation's commercial airports, either through new activities or by enhancing ongoing efforts. (For a list of ongoing efforts TSA initiated prior to 2009 to oversee and facilitate airport security, see app. III.) Since we last reported on airport security in September 2009, TSA has taken steps to develop strategic goals and evaluate risks, enhance aviation worker screening efforts, develop airport planning and reference tools, and assess general airport security through the review and feedback of aviation stakeholders and experts.[55] According to TSA officials, these actions have reinforced the layers of security already in place to stop a terrorist attack.[56] The following are two actions that, according to TSA officials, have played an important role in facilitating airport perimeter and access control security.

- **Aviation Security Advisory Committee (ASAC) recommendations.** In January 2015, in the wake of the December 2014 Atlanta gun-smuggling event allegedly perpetrated by current and former airline workers, the TSA Acting Administrator requested that ASAC—a TSA advisory committee—evaluate employee access

[55] GAO-09-399.

[56] While many of the layers of security apply directly to airport perimeter and access control security, some apply to other aspects of aviation security, such as hardened cockpit doors, and also to the security of other modes of transportation, such as rail and mass transit. According to TSA officials, each of the security layers is capable of stopping a terrorist attack, but used in combination they form a much stronger security system.

control security at commercial airports.[57] In response, ASAC created the Working Group on Airport Access Control (Working Group), composed of various industry experts and supported by officials from TSA and the Homeland Security Studies and Analysis Institute—a federally funded research and development center—to analyze the adequacy of existing airport employee access control security measures and recommend additional measures to improve worker access controls.[58] In April 2015, the Working Group issued a report on potential vulnerabilities related to airport employee access control security and the insider threat, recommending 28 actions to be taken across five areas: (1) security screening and inspection, (2) vetting of employees and security threat assessment, (3) internal controls and auditing of airport-issued credentials, (4) risk-based security for higher-risk populations and intelligence, and (5) security awareness and vigilance.[59] TSA fully concurred with 26 of the 28 recommendations and partially concurred with 2.[60] As of August 2015, TSA officials reported that the agency had implemented—closed—6 of the 26 recommendations they concurred with and had established timeframes for addressing the remaining 20 recommendations, the last of which TSA anticipates implementing in 2018. According to these officials, TSA will need to form working groups to respond to some recommendations and may find that some recommendations

[57] 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 nine stakeholder groups affected by aviation security requirements. The Aviation Security Stakeholder Participation Act of 2014, enacted in December 2014, required that an aviation security advisory committee be established and specifically required the establishment of a subcommittee to address, among other issues, perimeter and access controls. See Pub. L. No. 113-238, 128 Stat. 2842 (2014) (codified at 49 U.S.C. § 44946).

[58] See, e.g., 6 U.S.C. § 192 (requiring the Secretary of DHS to establish a federally-funded research and development center, which it established in March 2009).

[59] According to the ASAC report, the Working Group based its analysis on a model that followed the flow of typical airport employment and credentialing practices: pre-employment vetting, badging, and worker practices such as arriving and leaving work, entering secured areas, and performing daily activities. The Working Group segmented the model into the five operational areas of analysis and generated recommendations for each area.

[60] According to TSA officials, the agency could not fully concur with one recommendation due to statutory limitations and the second due to actions needed at the airport level.

are infeasible. In September 2015, ASAC also issued six recommendations for addressing commercial airport perimeter security vulnerabilities. These recommendations cover four areas of action: (1) adopt select industry best practices (e.g., joint assessments of airport perimeter risk), (2) institute an airport security-focused grants program, (3) incorporate risk-based security into airport security requirements, and (4) embed perimeter security awareness training in annual airport security refresher training for aviation workers. TSA fully concurred with these recommendations. As of February 2016, TSA reported that the agency had established timeframes for addressing the recommendations, with the last recommendation to be implemented by the end of 2016.

- **Playbook.** In March 2015, TSA refocused "Playbook," a risk-based program that authorizes FSDs to carry out random, unpredictable combinations of security operations at all areas of an airport to address real-time threats and to deter potential terrorist attacks.[61] Playbook consists of a menu of predefined "plays"—operations that identify specific resources, activities, locations, and targets—that FSDs or TSA headquarters officials can manually or randomly select using a randomization tool.[62] The plays are conducted by teams of TSA and non-TSA personnel. Historically, while TSA headquarters mandated that Playbook operations be conducted at specific airports, generally it allowed FSDs—in coordination with airport operators—to

[61] According to TSA officials, Playbook was implemented in December 2008 and evolved from gate screening of high-risk flights and the Aviation Direct Access Screening Program (ADASP)—an aviation worker screening program that was used from August 2006 through December 2009 to enforce access procedures, such as ensuring workers displayed appropriate credentials and did not possess unauthorized items. ADASP was conducted on an unpredictable basis and included temporary worker screening checkpoints, vehicle screening checkpoints, or both. In March and April 2015, TSA expanded the Playbook staffing allocation model to include 12 baseline insider threat risk factors.

[62] According to TSA officials, the agency used risk-based threat and vulnerability matrixes to tailor plays to align with the top airport threats (identified through the TSSRAs) and the top vulnerabilities (identified through JVAs).

determine which plays to conduct.[63] However, since March 2015, in response to the December 2014 Atlanta gun-smuggling event allegedly perpetrated by current and former airline workers, TSA headquarters has directed that a high percentage of Playbook operations focus on the insider threat, primarily through the random screening of workers, property, and vehicles.[64] According to TSA data, from June 1 through June 30, 2015, Playbook operations identified 50 worker-related security events, such as workers attempting to gain unauthorized access to a security-restricted area, workers attempting to gain access to a restricted area with expired credentials, and workers with prohibited items.[65]

Since 2009, TSA has also developed plans for assessing and responding to risks, programs to address worker security issues, tools for airports to assess and respond to risks, guidance and reference tools for airports, and general security activities. Table 2 lists additional actions TSA has taken since 2009 in relation to perimeter and access control security.

[63] Prior to April 2015, TSA headquarters allocated a specific number of full-time equivalent (FTE) positions to specified airports to conduct mandatory Playbook operations. In fiscal year 2015, a certain number of airports received FTEs to conduct mandatory Playbook operations. FSDs overseeing TSA operations at other airports (non-mandatory airports) were allowed to use their discretion in determining the amount of FTEs to expend on Playbook operations, with the resources coming from their general allocations. FSDs overseeing non-mandatory airports could choose not to carry out Playbook operations.

[64] TSA determined the specific percentage of Playbook operations focused on the insider threat to be SSI. Therefore, we do not identify the specific percentage.

[65] Pursuant to TSA requirements, airport workers who require an item for the performance of their assigned duties, but that is otherwise prohibited from being carried into the sterile area of an airport, may possess and use the item in the sterile area but may not take the items through the passenger screening checkpoint. Items that are prohibited to aviation workers in one security-restricted area may not be prohibited in another. Prohibited items can include, but are not limited to, ammunition, firearms, knives, tools, sporting goods—such as baseball bats—and explosives. In one of the above security events, TSA officers, conducting "open and look" bag searches of workers at an airport's direct access point, selected a worker for additional screening and found a stun gun—a prohibited item—in his personal property. During "open and look" bag searches at a different airport, TSA officers found bundles of cash—not a prohibited item—in a worker's personal property. In this case, TSA officers suspected illegal activity and referred the worker to law enforcement.

**Table 2: Additional Airport Perimeter and Access Control Security-Related Actions the Transportation Security Administration (TSA) Has Initiated since 2009**

| Type of security action | TSA action and date initiated | Description |
|---|---|---|
| Risk planning and assessment | *National Strategy for Airport Perimeter and Access Control Security* – 2012 | In response to our 2009 recommendation, TSA developed a national strategy for airport perimeter and access control security.a This strategy includes, among other things, strategic goals and objectives such as promoting the use of innovative and cost effective measures for reducing risk to airport perimeter and controlled access areas. |
| | *Comprehensive Risk Assessment of Perimeter and Access Control Security, Sensitive Security Information* (SSI) – 2013 | In response to our 2009 recommendation, TSA used existing threat, vulnerability, and consequence assessment information to develop a risk assessment specifically related to airport perimeter and access control security.[a] |
| Worker security programs | *This is My Airport* - 2015 | *This is My Airport* is a training program for airport, tenant, and contractor employees with airport-issued credentials, designed to raise security awareness through worker commitment to mission, workplace vigilance, and detection and reporting of suspicious activity at their airport. According to TSA officials, TSA and transportation security stakeholders have also implemented the Department of Homeland Security's (DHS) "If You See Something, Say Something" program and similar security awareness programs as local initiatives. |
| | FBI Rap Back - 2015 | The Federal Bureau of Investigation (FBI) Rap Back program uses the FBI fingerprint-based criminal records repository to provide recurrent fingerprint-based criminal history record checks for aviation workers who have been initially vetted and already received airport-issued identification credentials. As of October 2015, TSA was in the initial stages of planning for the piloting of the program, with two airports and one airline planned for enrollment. |
| Airport security planning and assessment tools | *Self-Vulnerability Assessment Tool* (SVAT) (SSI) - 2010 | According to TSA officials, the SVAT is a self-inspection tool that TSA provides to airports in advance of a joint vulnerability assessment (JVA) to help JVA teams identify vulnerabilities in preparation for the vulnerability assessment. |
| | *Commercial Airport Resource Allocation Tool* (CARAT) (SSI) - 2010 | Developed in October 2010, TSA designed CARAT for airport operators to perform their own internal risk assessment and resource allocation evaluations by estimating returns on investment of current and proposed security measures. It is available to airports through TSA's internet Web Board. |
| | *Airport Security Self-Evaluation Tool (ASSET) Users' Guide* (SSI) - 2011 | Deployed in May 2011, ASSET allows airports to evaluate their airports' current levels of security compared to other domestic airports. ASSET is available to airports through TSA's internet Web Board. |
| Airport guidance and reference materials | RTCA, Inc., guidance – 2011 and 2013 | As a member of the RTCA, Inc., a federal aviation advisory committee formerly known as the Radio Technical Commission for Aeronautics, TSA worked with primary aviation stakeholders on the RTCA, Inc.'s Special Committee on Airport Security Access Control Systems to develop guidance and standards for access controls at airports, including specifications for access control technologies. As this is a permanent committee, TSA and other members are to conduct ongoing revisions to standards and guidance as needed. |

| Type of security action | TSA action and date initiated | Description |
|---|---|---|
| | *Commercial Airport Innovative Security Measures* (SSI) - 2011 | A compendium of innovative (best practice) security measures—defined as measures exceeding minimum government standards or meeting standards in a unique manner—employed at various commercial airports. TSA developed this compendium to increase airport operators' awareness of innovative security measures at various airports and to provide them with information regarding the cost and operational implications of those measures. The measures in this report also provide the basis for the development of ASSET and CARAT, and are available to airports through TSA's internet Web Board. |
| | *Biometrics Use for Access Control and Credentialing at U.S. Commercial Airports* (SSI) - 2012 | In 2011, TSA asked the Homeland Security Studies and Analysis Institute to research the use of biometrics for commercial airport access control and credentialing to, according to TSA, inform a more unified approach for biometrics implementation across the industry.[b] The resulting 2012 report describes early adopters' experiences with biometrics in both airport and non-airport environments, and is to serve as a reference for airport operators and TSA policy makers. |
| | *Airport Security Program and 49 CFR 1542 Implementation Guidance* (SSI) – 2014 | This guidance is intended to assist airport operators, federal security directors (FSD) and staff in meeting the regulatory requirements under 49 C.F.R. Part 1542 when developing, modifying, or approving airport security programs (ASP). This document provides guidance to operators of category X through IV airports for addressing applicable regulatory requirements. |
| General airport security | Quarterly Airport Security Review (formerly known as "In-Depth Security Review") - 2009 | In response to our 2009 recommendation, TSA and select industry associations formed a working group—the In-Depth Security Review—to review all active security directives (SD) and security program amendments to consider the placement of these requirements within the regulatory framework, to include deletions or revisions to current requirements.[a]<br>In January 2015, TSA renamed the In-Depth Security Review to the "Quarterly Airport Security Review"; according to TSA officials, the function has not changed although the focus is now geared toward current security issues and their solutions. |
| | Compliance Security Enhancement Through Testing (COMSETT) - 2014 | COMSETT is an airport and airline compliance testing procedure that uses a three-phased approach to testing: (1) test for compliance without enforcement penalty for failure, (2) employ risk mitigation and outreach efforts to identify the causes of failed testing and share best practices identified through successful testing, and (3) retest to determine if failure rate improves. According to TSA officials, absent significant egregious or aggravating circumstances, penalties for failed tests are not imposed until airports have been given an opportunity to address compliance issues. |
| | Security Directives (SD) (SSI) – 2015 | In 2015, as a result of Aviation Security Advisory Committee (ASAC) recommendations for addressing insider threat issues, TSA updated an existing SD to require airport operators to conduct fingerprint-based criminal history records checks every 2 years for all workers with airport-issued credentials (badges). TSA updated another SD to require that airport operators notify individuals with airport-issued credentials who are traveling as passengers that they must access the sterile area through the TSA security checkpoint. |

| Type of security action | TSA action and date initiated | Description |
|---|---|---|
| | Information Circulars (SSI) – 2015 | In 2015, in response to ASAC recommendations for addressing insider threat issues at commercial airports, TSA issued Information Circulars, which encouraged airports to:<br>• reduce the number of access points to security-restricted areas to the operational minimum (as required by a pre-existing national airport security program amendment and other policies);<br>• provide recommendations, suggested procedures, and minimum frequency standards for random, physical aviation worker inspection; and<br>• increase the detection and reporting of insider threat activity by airport workers. |
| | Centralized Security Vulnerability Management Process – 2015 | As of December 2015, TSA was in the early stages of developing an agency-wide process for reporting, assessing, addressing, and monitoring identified security vulnerabilities. According to TSA, this process is to apply to all evaluations, assessments, and testing of security vulnerabilities, such as covert "Red Team" and Aviation Screening Assessment Program testing; JVAs; Man-Portable Air Defense Vulnerability Assessments; inspections of TSA operations; investigations of employee misconduct and employee fraud; and Mission, Asset, and System Specific Risk Assessments, among other things.[c] |

Source: GAO analysis of TSA data. I GAO-16-632

[a] 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).

[b] The Secretary of DHS established the Homeland Security Studies and Analysis Institute in March 2009. See 6 U.S.C. § 192 (authorizing the Secretary to establish a federally funded research and development center). Biometrics are measurements of an individual's unique characteristics, such as fingerprints, irises, and facial characteristics, used to verify identity.

[c] According to TSA, the agency developed this new process because existing processes for evaluating and managing identified vulnerabilities are not centralized and do not ensure the level of visibility and accountability needed to ensure appropriate response and closure. Specifically, the 2015 root causes analysis into checkpoint covert test failures identified TSA's processes for tracking and managing closure of identified security vulnerabilities as an organizational deficiency.

## TSA Developed a National Strategy to Guide Oversight of Airport Security, but Has Not Updated It to Reflect Changes in Its Risk Assessment of Airport Security and Other Actions

TSA has not updated its September 2012 *National Strategy for Airport Perimeter and Access Control Security* (Strategy) to reflect actions it has subsequently taken to assess the airport security risk environment, oversee and facilitate airport security, and address Strategy goals and objectives. The Strategy, which TSA developed in response to our 2009 recommendation,[66] defines how the agency seeks to secure the perimeters and controlled areas of the nation's commercial airports.[67] As previously discussed in this report, TSA has addressed a key objective of its Strategy by developing the 2013 Risk Assessment of Airport Security, which assesses the airport security risk environment based on the 2013 TSSRA, 2011 JVA information, and a 2012 Special Emphasis Assessment. However, it has not updated the Strategy with the results of this assessment, such as vulnerability information from JVAs, results from the Special Emphasis Assessment, and the direct and indirect consequences of various attack scenarios. Further, it has not updated the Strategy with threat information from the July 2014 and 2015 versions of the TSSRA, including assessments of the risk from the insider threat and how TSA plans to address that risk, as well as the results of JVAs conducted since 2013.[68]

TSA also has not incorporated information on key airport security activities it has developed or enhanced since 2009. Two such efforts include Playbook and COMSETT, programs TSA officials have stated are key to addressing airport security risk. Additionally, TSA has not updated

[66] GAO-09-399.

[67] The TSA-issued Strategy is defined as an overarching framework for setting and communicating goals and priorities for airport security and for allocating resources to inform decision making and help ensure accountability. Additionally, the Strategy is to help link individual programs to specific goals and describe how the programs will contribute to achieving those goals. The Strategy identifies the following three high-level security goals: (1) prevent and detect perimeter breaches and unauthorized access into secured areas of the nation's commercial airports, (2) promote the use of innovative and cost-effective measures for reducing risk to airport perimeter and controlled access areas, and (3) enhance stakeholder coordination to integrate airport perimeter and access control programs with other aviation security priorities. The Strategy also states TSA's intent to identify outcome-based performance targets and performance levels for each strategic goal once a comprehensive airport security risk assessment has been completed.

[68] As previously discussed, the July 2014 and July 2015 versions of the TSSRA sent to Congress were updated by TSA to include additional attack scenarios and reflect an increase in threat scores across all modes of transportation. Furthermore, TSA expanded the TSSRA in the 2014 and 2015 versions to assess risk from the insider threat.

the Strategy with the status of its efforts to address various goals and objectives. For example, TSA's second Strategic goal is to "promote the use of innovative and cost effective" actions for reducing risk. TSA has worked with industry representatives to identify a list of airport innovative (best practice) security measures that airports have implemented, as well as their associated costs and operational effects. The agency has also developed tools that allow airports to compare their security levels against those of other domestic commercial airports and to weigh expected costs associated with alternative security activities against expected benefits. However, TSA has yet to incorporate these developments into its Strategy.

TSA also has not updated the Strategy with the status of its efforts to identify outcome-based performance measures and performance levels—or targets—for each strategic goal, against which progress can be measured, as promised in its Strategy.[69] TSA proposed outcome-based performance measures in the Strategy for some activities, such as assigning vulnerability scores for each airport that receives a JVA, but did not identify performance targets against which progress can be measured.[70] Moreover, TSA has not updated the Strategy with outcome-based performance measures and performance targets for other airport security-related activities, such as Playbook and COMSETT. In addition to not having measures or targets, TSA also does not have a process in place for determining when additional updates to the Strategy are needed.

As we have previously reported, effective strategic plans are the foundation for defining what an agency seeks to accomplish and provide an overarching framework for communicating goals and priorities,

[69] In the Strategy, TSA describes airport security performance measures as "primarily based on output-based indicators that do little to measure the effectiveness of protection and mitigation activities."

[70] According to the Strategy, TSA would use JVA data to weigh, analyze, and convert specific airport vulnerabilities to a score for each TSSRA attack scenario (high, medium, low). Each airport would then receive a vulnerability score that assessed security and recorded observations of specific vulnerabilities in each of five core components—perimeter, operations, services, terminal, and infrastructure. Vulnerability scores would be based on a 4-point scale—from 1 (minor) to 4 (critical). Airports with a high score—the target level to be defined—would be flagged to receive measures to mitigate specific vulnerabilities.

allocating resources to inform decision making, and ensuring accountability.[71] Strategic plans, with their goals and objectives, are also the first phase in the risk management framework, which, according to the NIPP, is to be a continuing process with iterative steps and feedback loops that share information—such as identified threats and vulnerabilities—within each element of the framework and allows decision makers to track progress and implement actions to improve security over time. Further, our prior work has shown that leading organizations use acquired knowledge and data—such as information from new activities—to report on their performance.[72] The NIPP and other federal guidance also provide that agencies should assess whether their efforts are effective in achieving key security outcomes so as to help drive future investment and resource decisions and adapt and adjust protective efforts as risk changes.[73] In addition, *Standards for Internal Control in the Federal Government* states that as programs change, management must continually assess and evaluate its internal control to assure that the control activities being used are effective and updated when necessary.[74]

TSA officials stated that as of October 2015 the Strategy had not been updated to reflect the most recent Risk Assessment of Airport Security information, new airport security-related activities, the status of goals and objectives, and outcome-based performance measures and finalized performance levels (targets) for each strategic goal. These officials agreed that updating the Strategy with this information could be useful in guiding TSA's future airport security actions. They also stated that while they have developed output-based performance measures for many airport security-related activities and programs, they have yet to develop outcome-based performance measures and targets for these programs

[71] GAO-09-399.

[72] GAO, *Executive Guide: Effectively Implementing the Government Performance and Results Act*, GAO/GGD-96-118 (Washington, D.C.: June 1996).

[73] Internal control standards and GPRAMA also call for agencies to have measures and indicators linked to mission, goals, and objectives to allow for comparisons to be made among different sets of data (for example, desired performance against actual performance) so that corrective actions can be taken if necessary. See GAO/AIMD-00-21.3.1; Pub. L. No. 111-352, § 3, 124 Stat. at 3867-71 (codified at 31 U.S.C. § 1115); and Office of Management and Budget Circular No. A-11, Part 6, Preparation and Submission of Strategic Plans, Annual Reports.

[74] See GAO/AIMD-00-21.3.1.

and other activities—including Strategy goals—due to resource and time constraints. Further, TSA officials stated that the agency does not have a process in place for determining when updates to the Strategy are needed. TSA's Chief Risk Officer also agreed that TSA's oversight of airport security could benefit from an updated Strategy, and noted that the agency is in the process of developing the Strategic Operational Vision, a 5- to 7-year national strategy that is to address TSA-planned actions for aviation security; the strategy is scheduled to be released in February 2016. However, the official could not say to what extent the national strategy will address perimeter and access control issues. TSA officials stated in February 2016 that they agreed the Strategy should be updated, and plan to revise it to reflect actions the agency has taken since 2012 to assess the airport security risk environment, oversee and facilitate airport security, and address Strategy goals and objectives. Officials said they did not yet have milestones or a timeframe for completing the update, however, and had not yet conducted analysis to identify the status of goals and objectives or developed targeted performance levels for relevant programs, among other things.

Updating the Strategy to reflect changes in the airport security risk environment as well as new and enhanced activities TSA has taken to facilitate airport security would help TSA to better inform management decisions and focus resources on the highest-priority risks, consistent with its strategic goals. Further, updating the Strategy to identify the extent to which TSA has achieved goals and objectives would also help the agency to better assess its progress and manage limited resources to focus on areas that potentially require more attention and development. Developing outcome-based performance measures and targets, as required by the NIPP, would also allow TSA to assess to what extent it has achieved security goals and objectives so as to help drive future investment and resource decisions as well as adapt and adjust security efforts as risks change. TSA could also use performance measurement information to help it better identify problems or weaknesses in individual programs and activities as well as the factors causing those problems. Furthermore, establishing a process for determining when additional updates to the Strategy are needed would help to ensure that the Strategy contains the most up-to-date and relevant information for guiding TSA decision making related to airport perimeter and access control security.

## Selected Commercial Airports Have Taken a Variety of Approaches Intended to Strengthen Perimeter and Access Control Security

The 11 commercial airports we contacted have taken a variety of technology- and nontechnology-based approaches since 2009 to strengthen perimeter and access control security, and have encountered challenges related to cost and effectiveness in implementing these approaches.[75] According to airport officials, as well as representatives from industry and specialist organizations, there is no single "best" approach to securing airports against intrusion.[76] Rather, what works best for one airport often may not work for others—each airport is unique in its combination of layout, operations, and the security approaches and methods airports employ, according to these officials. For example, size—both acreage and operations—and available resources vary across airports and play a prominent role in determining the type of security approaches and methods an airport operator employs.[77] Other differentiating factors can include environmental surroundings, individual airport characteristics, previous security events, and airport category.[78] To help them assess these factors and choose the best security approach from the multiple security options available to them, airport operators can, among other things, contract with a private consultant or consult with National Safe Skies Alliance, Inc., who may conduct operational testing of

[75] We visited or interviewed officials at 11 selected commercial airports. Some of the examples of airport activities cited were started prior to 2009, but all were finalized or expanded after 2009.

[76] We interviewed officials from two industry associations—AAAE and ACI-NA—and two specialist non-profit organizations—National Safe Skies Alliance, Inc., and RTCA, Inc.—based on input from TSA officials and airport officials and the associations' specialized knowledge and experience with airport security operations.

[77] The airports we contacted ranged in size from "small"—with a 5-6 mile perimeter, 1 terminal, 1 boarding gate, and 30 badged workers—to "large"—with a 37-mile perimeter, 7 terminals, over 200 boarding gates, and approximately 60,000 badged workers. "Available resources" includes human capital resources as well as funding—for example, workers at a smaller airport often have multiple duties and staff utilization can be a key concern for officials when considering airport security options.

[78] "Environmental surroundings" refers to the surrounding environment, such as terrain—swamp, woods, etc.—and geography—water barriers, dense urbanization, etc. For example, airport operators in busy metropolitan areas where vehicles may be driven nearby, may employ a jersey barrier at the bottom of the fence to withstand a higher velocity crash threat. "Individual airport characteristics" refers to unique or individualistic features that can impact security considerations. For example, one airport we contacted is collocated with military operations. "Previous security events" refers to the impact security events can have on airport operators' security decisions. For example, a high-profile event might prompt an operator to consider more comprehensive security measures.

aviation security procedures, technologies, or systems on their behalf. Airport operators we contacted characterized their security approaches and methods as either technology- or nontechnology-based. Below are examples of the approaches these airport operators have taken after 2009 as well as the associated challenges.

**Technology-based approaches to airport security.** Airport operators stated they use a range of technology to varying degrees to enforce airport security. The types of technology airports employ can range from badge readers, to much more costly and sophisticated multi-faceted systems, such as perimeter intrusion detection systems (PIDS).[79] With respect to access control security, all 11 of the airport operators we contacted use badge readers to control access to security-restricted areas and some require a personal identification number to gain access to security-restricted areas. One of the airport operators reported using technology to guard against the use of fraudulent credentials by embedding special technology in workers' identification badges to verify authenticity. Airport operators also reported using a range of technologies to secure perimeters, from closed-circuit television cameras and fence sensors to PIDS. Generally, larger airports reported testing more pilot technologies and using more sophisticated technology, such as biometric readers (e.g., finger print and hand geometry scanners), PIDS, anti-piggybacking systems,[80] and mobile surveillance towers,[81] among other things. (See fig. 4 for an image of a mobile surveillance tower at a commercial airport.) However, one smaller airport operator we contacted has deployed sophisticated technology to strengthen its perimeter and

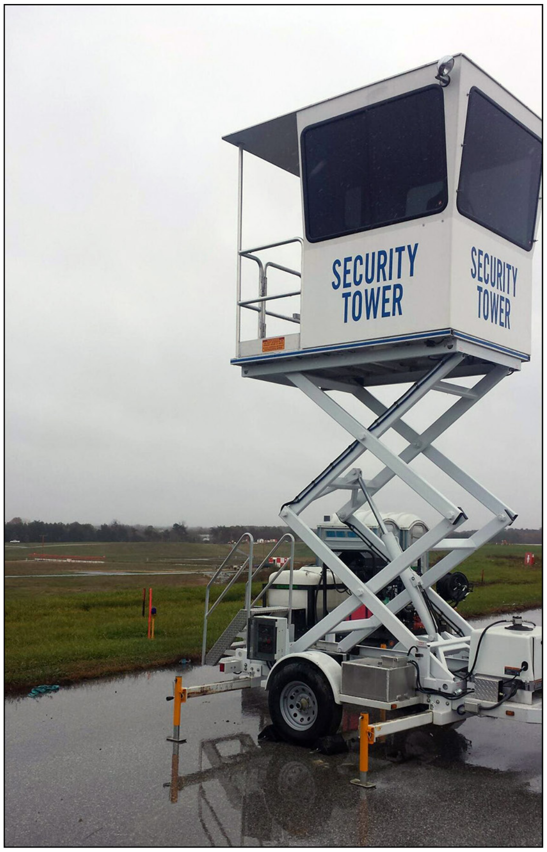
[79] Perimeter intrusion detection systems (PIDS) are multi-faceted systems that can employ radar, video motion detection, infrared cameras, and fence sensors, among other things.

[80] Piggybacking occurs when an unauthorized individual, on foot or in a vehicle, enters through a portal providing access to a sterile area, secured area, SIDA or AOA during an authorized individual's entry into or exit from such area with or without the authorized person's knowledge. Piggybacking also occurs when an otherwise authorized individual accesses an open secured area, SIDA or AOA portal without following required access control procedures.

[81] Mobile surveillance towers are portable towers that can employ integrated thermal imaging, high-definition cameras, long-range color video, and video analytics, among other things, and are used to monitor large areas such as an airport parking lot or perimeter.

access controls, and more readily detect unauthorized access to security-restricted areas.

Figure 4: Mobile Surveillance Tower at a Commercial Airport



Source: Baltimore-Washington International Thurgood Marshall Airport. | GAO-16-632

Airport officials cited cost and limitations in system effectiveness as challenges to using technology to enhance airport security. According to airport and industry association officials, and representatives from specialist organizations, the cost of installing, maintaining, and upgrading technology can be a significant challenge to implementing even relatively simple technology as well as more sophisticated detection systems. For example, one large airport operator reported spending approximately $40 million in updating its security platform with additional cameras, active shooter alarms, and card readers. Officials from three airports said that they would like to implement biometrics as another layer of access control security, but are concerned about installation, maintenance, and update costs. One airport operator reported spending at least $1 million to install biometric technology at selected access portals, and another spent approximately $3 million to update its credentialing system. Officials also cited limitations in technology effectiveness as another significant challenge—for example, in certain situations perimeter systems may report too many false positives for effective use.[82] Officials also noted that system performance can vary. For example, perimeter technology may not function effectively without modification in certain environmental conditions.[83] Airport and industry officials also noted that the human factor can play a significant role in the effectiveness of many security technologies because the systems require human monitoring to interpret and respond to alarms—if the systems register too many false alarms, personnel may eventually ignore alarms, even potentially valid ones.

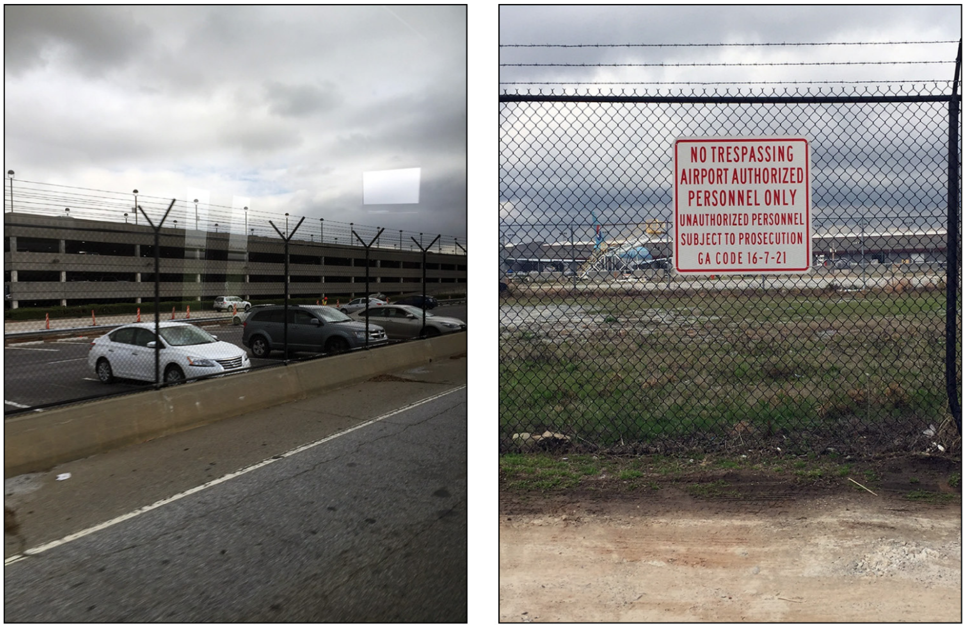
**Nontechnology-based approaches to airport security.** Airport and industry officials stressed that technology is not always the best or only option for ensuring airport security, given the individual needs of the airport. Airport officials said they use a variety of nontechnology tools and techniques to secure their perimeters, such as fences, crash barriers, law enforcement patrols, and security buffer zones, among other things (see fig. 5 for fencing used by one airport to secure its perimeter). Four airport operators told us they have law enforcement or contract personnel continuously patrolling their perimeters, while two operators said they maintain three-and ten-foot buffer zones on both sides of their perimeter fence to better detect intruders. Two airport operators with water perimeters said they address the potential threat of boaters breaching their perimeters by implementing security zones ranging from 100 to 300 feet from their perimeters. Airport operators said they also use nontechnology techniques to monitor access to security-restricted areas—for example, aviation workers are required to establish “challenge programs” that train aviation workers to identify potential threats, such as individuals without visible badges. Airport operators also reported

[82] TSA determined the specific situations that may result in false positive reports to be SSI. Therefore, we do not identify the specific situations that may produce false positive reports.

[83] TSA determined the specific environmental conditions under which perimeter technology may not function effectively to be SSI. Therefore, we do not identify those conditions.

conducting random worker screening activities to check aviation workers for prohibited items prior to their entering security-restricted areas. In response to the alleged gun smuggling event by current and former airline workers at the Atlanta Hartsfield-Jackson International Airport (i.e., the insider threat), one airport operator recently implemented full worker screening and another operator is in the process of implementing full worker screening.[84]

Figure 5: Example of Airport Perimeter Fence



Source: GAO. | GAO-16-632

[84] The airport operators we contacted described "full worker screening" as the physical screening or inspection of "most" aviation workers who work at an airport and require access beyond public areas, such as vendor, airport, air carrier, and maintenance employees. According to these officials, full worker screening exempts certain aviation workers such as law enforcement personnel from screening. Also according to these officials, full worker screening does not include the same tools and procedures as those used for passenger screening. TSA also conducts random worker screening through Playbook.

Airport officials and representatives from a specialist organization cited cost as a significant challenge to using various nontechnology approaches to enforce airport security. For example, officials at one airport estimated that implementing full worker screening will cost approximately $35 million in the first year and $10 million annually thereafter.

## Conclusions

Recent security events have highlighted the vulnerability of commercial airports to weaknesses in perimeter security and insiders who are intent on using their access privileges to commit criminal and potential terrorist acts. Since 2009, TSA has taken steps to strengthen the security of airport perimeters and access controls through enhanced requirements, oversight, and guidance, and through the development of a risk assessment that focuses on risks to airport security. Ensuring TSA's Risk Assessment of Airport Security is based on current threat and vulnerability information that reflects the pressing concern of the insider threat, as well as the most recent, known security vulnerabilities, would help TSA ensure that its limited resources are appropriately focused on the highest-priority risks. Moreover, sharing this relevant risk information with airport stakeholders would not only enhance their situational awareness but potentially allow them to make more informed decisions regarding airport security. Establishing a process for determining when additional updates to the Risk Assessment of Airport Security are needed and ensuring they are developed would ensure that TSA's mechanism for assessing risks to perimeter and access control security appropriately reflects changes in the risk environment.

As we reported in 2009, given TSA's position that the interconnected commercial airport network is only as strong as its weakest asset, determining airport security vulnerability across the network is fundamental to determining the actions and resources that are necessary to reasonably protect it.[85] Assessing the vulnerability of airport security system-wide would help TSA ensure that it has comprehensively assessed risks to commercial airports' perimeter and access control security. Given budget and resource constraints, it might not be feasible to assess the vulnerability of the nation's approximately 440 commercial

[85] GAO-09-399.

airports individually, but other approaches—such as assessing a sample that reflects a broader representation of airports or providing airports with a self-vulnerability assessment tool—would provide a system-wide perspective on vulnerability while requiring fewer resources.

The assessment of relevant data, including event data that may identify system-wide trends in airport security vulnerabilities and potential threats to airport security, is integral to risk-based decision making. Analyzing relevant data would help TSA to identify relevant trends in perimeter and access control security as well as improve the agency's understanding of risk.

In response to our 2009 recommendation, TSA developed a strategy to guide and unify the agency's efforts to strengthen airport security.[86] However, if the Strategy does not incorporate the most current assessment of airport security-related risk and new activities TSA has taken to facilitate airport security, its value as a decision-making tool may not be fully realized. Updating the Strategy to reflect TSA's progress in addressing relevant goals and objectives would also help TSA to identify areas that potentially require more attention and a greater share of resources. Perhaps most importantly, the development of outcome-based performance measures and targets would better enable TSA to assess the extent to which its activities have been effective, and allow it to more effectively adapt security efforts as risks evolve. Establishing a process for identifying when updates to the Strategy are needed and ensuring they are developed would ensure that TSA has the most relevant and current information available for airport security to guide its decision making.

## Recommendations for Executive Action

To help ensure TSA's actions in overseeing and facilitating airport security are based on the most recent available risk information that assesses vulnerabilities system-wide and evaluates security events, and that these actions are orchestrated according to a strategic plan that reflects the agency's goals and objectives and its progress in meeting those goals, we recommend that the Administrator of TSA take the following six actions:

[86] GAO-09-399.

- Update the Risk Assessment of Airport Security to reflect changes to its risk environment, such as those updates reflected in TSSRA and JVA findings, and share results of this risk assessment with stakeholders on an ongoing basis.
- Establish and implement a process for determining when additional risk assessment updates are needed.
- Develop and implement a method for conducting a system-wide assessment of airport vulnerability that will provide a more comprehensive understanding of airport perimeter and access control security vulnerabilities.
- Use security event data for specific analysis of system-wide trends related to perimeter and access control security to better inform risk management decisions.
- Update the 2012 Strategy for airport security to reflect changes in risk assessments, agency operations, and the status of goals and objectives. Specifically, this update should reflect
  - information from the Risk Assessment of Airport Security, as well as information contained in the most recent TSSRA and JVAs;
  - new airport security-related activities;
  - the status of TSA efforts to address goals and objectives; and
  - finalized outcome-based performance measures and performance levels—or targets—for each relevant activity and strategic goal.
- Establish and implement a process for determining when additional updates to the Strategy are needed.

## Agency Comments and Our Evaluation

We provided a draft of this report to DHS for their review and comment. DHS provided written comments, which are noted below and reproduced in full in appendix IV; these comments include information regarding TSA's planned actions that was not included in the prior sensitive report. TSA also provided technical comments, which we incorporated as appropriate.

DHS concurred with all six recommendations in the report and described actions underway or planned to address them. With regard to the first recommendation that TSA update the Risk Assessment of Airport Security, DHS concurred and stated that in March 2016 the agency established a National Strategy for Airport Perimeter Access Control Working Group (NSAPAC-WG), comprised of various TSA offices, to begin updating the Risk Assessment of Airport Security. This update is to include new data from various TSA programs and assessments, including the TSSRA and JVAs, with the goal of sharing nationwide best practices for mitigating airport perimeter and access control security vulnerabilities with airport operators. TSA expects to complete the update by April 30, 2017. This action, if implemented effectively, should address the intent of our recommendation.

With regard to the second recommendation to establish and implement a process for determining when additional risk assessment updates are needed, DHS concurred and stated that TSA plans to initiate updates to the Risk Assessment of Airport Security once every 3 years. TSA stated that this timeframe is needed to allow for an extended schedule of JVAs and other source material and for analysis of mature data to identify consistencies and changes and provide that analysis to airport operators. DHS reported that the NSAPAC-WG will be re-established every 3 years to lead these updates, which are to include a review of all newly collected data, assessments of policies implemented since the last risk assessment, and consideration of possible changes to the assessment. The NSAPAC-WG is to complete its review and revision of the assessment within 2 years of the start of the update. This action, if implemented effectively, could address the intent of our recommendation. However, it is not clear to what extent this process would address changing conditions outside the cycle that could require an immediate update or reexamination of risk. We will continue to monitor TSA's efforts.

With regard to the third recommendation that TSA develop and implement a method for conducting a system-wide assessment of airport vulnerability, DHS concurred and stated that TSA has begun to take steps to develop methods that will provide a more comprehensive understanding of airport security vulnerabilities. Specifically, TSA has asked airport operators to complete a vulnerability assessment checklist that focuses on perimeter and access control security, including the insider threat, and plans to direct its leadership in the field to work with airport operators to review the assessment results and develop and implement risk mitigation plans. In January 2016, TSA also began to implement the Centralized Security Vulnerability Management Process, an agency-wide process for identifying, addressing, and monitoring systemic security vulnerabilities. Additionally, TSA has organized the Compliance Risk Integrated Project Team, composed of various TSA offices, which focuses on identifying and addressing areas of greatest risk across all TSA-regulated parties, including airport operators. This program is to combine data from ongoing regulatory compliance processes—e.g., annual and targeted airport inspections, special emphasis assessments, inspector outreach, and response activities—

JVAs, a new Compliance Vulnerability Assessment program, and risk data to derive a Compliance Risk level. The resulting Compliance Risk level is to drive national, regional, and airport/facility deployment of TSA resources to address those areas identified as highest risk. DHS reported that the new Compliance Vulnerability Assessment component of this program is to draw on data from multiple sources, including JVAs, surface transportation baseline assessments, and cargo vulnerability assessments. According to DHS, as of May 2016, TSA had reviewed the security vulnerability assessments performed by airports in accordance with the vulnerability assessment checklist TSA earlier provided to airports, and is sharing the results of that review with airports and other appropriate stakeholders to support the development of risk mitigation plans. TSA plans to complete the entire compliance risk effort by September 30, 2018. This action, if implemented effectively, could address the intent of our recommendation but without examination of the documentation and underlying analysis it is too early to know. We will continue to monitor TSA's efforts.

With regard to the fourth recommendation to use security event data for specific analysis of system-wide trends related to perimeter and access control security, DHS concurred and stated that TSA held meetings in April 2016 to examine the analytic capabilities of SIRT to provide system-wide trends related to perimeter and access control security and consider the best use of this information to inform risk-based management decisions. According to DHS, TSA has identified specific SIRT data fields and designed analytical reports that are to be completed by July 31, 2016, and plans to use the results of the analysis to inform risk management decisions in fiscal year 2017. This action, if implemented effectively, should address the intent of our recommendation.

With regard to the fifth recommendation that TSA update its 2012 strategy for airport perimeter and access control security, DHS concurred and stated that TSA began updating the 2012 Strategy in January 2016 and in March 2016 turned the effort over to the newly created NSAPAC-WG. According to TSA, as of May 2016, the NSAPAC-WG has reviewed and compared the 2012 Strategy to the agency's operating environment, canvased subject matter experts to determine goals and objectives, and begun rewriting the strategy; TSA plans to complete the update by December 31, 2017. However, because the update will depend on finished analysis from the Risk Analysis for Airport Security, which must be received before the update to the Strategy can be completed, TSA plans to release an interim update to the Strategy by June 30, 2016. TSA also reported that it has released an Information Circular that encourages airport operators to conduct airport vulnerability assessments that focus on the insider threat and to use the results of the assessments to implement mitigation measures. TSA also plans to use the final update of the Strategy to introduce new and emerging threats and vulnerabilities that can impact perimeter and access control security, such as unmanned aerial systems and cyber security issues. This action, if implemented effectively, should address the intent of our recommendation.

With regard to the sixth recommendation to establish and implement a process for determining when additional updates to the Strategy are needed, DHS concurred and stated that TSA will implement a process similar to that for the Risk Assessment of Airport Security, in which the NSAPAC-WG will initiate updates to the Strategy once every 3 years. According to DHS, the updates are to include a review of all newly collected data, assessments of policies implemented since the last risk assessment, and consideration of possible changes to the strategy. The NSAPAC-WG is to complete its review and revision of the Strategy within 2 years of the start of the update. This action, if implemented effectively, could address the intent of our recommendation. However, it is not clear to what extent this process would address changing conditions outside the cycle that could require reconsideration of the Strategy. We will continue to monitor TSA's efforts.

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

If you or your staff have any questions, please contact me at (202) 512-7141 or groverj@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 significant contributions to this report are listed in appendix V.

Jennifer Grover

Jennifer Grover
Director
Homeland Security and Justice

*List of Requesters*

The Honorable Michael T. McCaul
Chairman
The Honorable Bennie G. Thompson
Ranking Member
Committee on Homeland Security
House of Representatives

The Honorable Cedric L. Richmond
Ranking Member
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
House of Representatives

The Honorable Bonnie Watson Coleman
Ranking Member
Subcommittee on Oversight and Management Efficiency
Committee on Homeland Security
House of Representatives

The Honorable Kathleen Rice
Ranking Member
Subcommittee on Transportation Security
Committee on Homeland Security
House of Representatives

The Honorable William R. Keating
House of Representatives

The Honorable Eric Swalwell
House of Representatives

# Appendix I: Objectives, Scope, and Methodology

This report addresses the Transportation Security Administration's (TSA) oversight of airport perimeter and access control security.[1] More specifically, our objectives were to examine (1) the extent to which TSA has assessed the components of risk—threat, vulnerability, and consequence—related to commercial airport perimeter and access control security since 2009; (2) the extent to which TSA has taken actions since 2009 to oversee and facilitate airport perimeter and access control security; and (3) the actions selected commercial airports have taken, if any, to strengthen perimeter and access control security since 2009.

For this report, we analyzed TSA's data on general airport security events from the Performance and Results Information System (PARIS)—TSA's system of record for regulatory activities and security events—from fiscal years 2009 (October 2008) through 2015 (September 2015).[2] We selected these timeframes to align with our 2009 report on airport perimeter and access control security and the last full fiscal year of data available at the time of our review.[3] TSA uses PARIS for maintaining information associated with TSA's regulatory investigations, security events, and enforcement actions across transportation modes, as well as for recording the details of security events involving passenger and property screening. Because TSA changed the security event reporting categories in PARIS and their definitions in October 2012, we analyzed data from fiscal years 2009 through 2012 separately from fiscal years 2013 through 2015. We selected event categories in PARIS that we

[1] According to TSA officials, "perimeter and access controls security" refers to the protection of airport perimeters (such as airfield fencing, vehicle access gates, and pedestrian access) and security features that control access to security-restricted areas of the airport, including baggage screening, sterile, cargo, catering, fuel farm, and other areas. Consistent with statements by TSA officials, the operational passenger checkpoint is not considered an access control for purposes of this report.

[2] TSA defines a "security breach" as any incident involving unauthorized and uncontrolled access by an individual or prohibited item into a sterile area or secured area of an airport that is determined by TSA to present an immediate and significant risk to life, safety, or the security of the transportation network which requires emergency response by law enforcement. TSA defines a "security incident" as an event that does not meet the criteria of a breach, but is reportable to PARIS as required by TSA's operations directive and guide. For the purposes of this report, a "security event" may be either a "security breach" or a "security incident."

[3] 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).

determined were most likely to contain events related to perimeter and access control security based on TSA's definitions. We further refined the data by removing those events that TSA identified as having occurred at an operational passenger screening checkpoint, which is specifically excluded from TSA's definition of perimeter and access control security. See table 3 for the categories and definitions we selected.

**Table 3: Selected Security Event Reporting Categories in Performance and Results Information System (PARIS) for Fiscal Years 2009 through 2015**

| PARIS event categories and definitions for fiscal years 2009 through 2012 | PARIS event categories and definitions for fiscal years 2013 through 2015 |
|---|---|
| Access control<br>Incidents involving a problem with secured entries, passages, or other means of access from within the airport to the airport's limited access areas, such as discovery of a secure door left open. | Access control – contained security incident<br>Any incident that involves an individual or item that gains access to the sterile or secured area and is under constant surveillance by airport security personnel or other trustworthy airport/security personnel until detained, and has been determined by the Transportation Security Administration (TSA) to NOT present immediate and significant risk to life, safety or the security of the transportation network. This category corresponds to the (former) PARIS incident type Perimeter Event. |
| Perimeter breach<br>Incidents where an unauthorized individual gains access to Air Operations Area (AOA)/security identification display area (SIDA) and is not under continuous surveillance—relates primarily to areas not associated with the TSA screening checkpoint operations.[a] | Access control – delayed resolution/no threat security incident<br>Any incident where the circumstances allow, or would allow, an individual or item to gain unauthorized access to a sterile, secure area or AOA and is not under continuous surveillance by airport/security personnel or other trustworthy airport/security personnel; and has been determined by TSA to NOT present immediate and significant risk to life, safety or the security of the transportation network. This corresponds to the (former) PARIS incident type Perimeter Event. |
| Perimeter event<br>Incidents where an unauthorized individual gains access to AOA/SIDA and is under constant surveillance by airport/security personnel until apprehended. | Security breach<br>Any incident involving unauthorized and uncontrolled access by an individual or prohibited item into a sterile area or secured area of an airport that is determined by TSA to present an immediate and significant risk to life, safety, or the security of the transportation network which requires emergency response by law enforcement. Events that do not meet these criteria are considered security incidents. |
| Security breach<br>Incidents involving an individual gaining access to the sterile area at the screening checkpoint or a collocated operational exit lane without submitting to all screening and inspections of his/her person and accessible property in accordance with procedures contained in the screening checkpoint standard operating procedures. | Stowaway<br>Incidents that involve individuals who obtain transportation aboard an aircraft (either passenger or cargo) without the consent of the aircraft operator, charterer, or person-in-command, through concealment. A passenger who boards with a valid ticket for a flight may not be considered a stowaway. |

Source: TSA operations directives for security incident reporting. | GAO-16-632

[a] In general, an AOA is an area providing access to aircraft movement and parking areas. A SIDA is an area in which appropriate identification must be worn, and may include the AOA as well as other secured areas of an airport.

These data consisted of the date on which the event occurred, the airport in which it occurred, the event category type as listed in table 3, and details of the event in narrative form, among other things. We assessed the reliability of the event data by (1) interviewing agency officials about the data sources, the system’s controls, and any quality assurance steps performed by officials before data were provided and (2) testing the data for missing data, duplicates, airports not regulated by TSA, values beyond expected ranges, or entries that otherwise appeared to be unusual. We identified a limitation in that data contain events that are not directly related to perimeter and access control security. For example, the “access control–contained security incident” category may include an event in which a police officer patrolling the terminal area observed a contractor’s unattended tools that may contain items prohibited in the sterile area. Further, other event categories that we did not include in our analysis may contain events that relate to perimeter and access control security. For example, we did not include event categories in our analysis, such as “disruptive individual,” “loss or theft of airport SIDA badge or access media,” or “suspicious individual or activity,” which may have included events related to perimeter and access controls security. We did not analyze the data to screen out unrelated events because that would require an extensive and resource-intensive content analysis of the event narratives to refine the records to include only those events that were specific to perimeter and access control security, and the narratives may not be sufficient to make an appropriate judgment. Therefore, the event data that we report may over- or under-represent the total number of events directly related to perimeter and access control security. However, with this caveat, we found the PARIS events data sufficiently reliable to provide descriptive information on the number of events potentially related to perimeter and access control security over fiscal years 2009 through 2015 and by airport category.[4]

[4] TSA classifies the nation’s approximately 440 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 largest number of passenger boardings and Category IV airports have the smallest.

To determine the extent to which TSA has assessed the components of risk—threat, vulnerability, and consequence—related to commercial airport perimeter and access control security since 2009, we analyzed documentation and data for TSA's risk assessment activities and interviewed TSA officials responsible for conducting these assessment activities. Specifically, we examined the extent to which TSA generally conducted activities intended to assess threat, vulnerability, and consequence at the nation's approximately 440 commercial airports. For all three elements of risk, we reviewed TSA's 2013 *Comprehensive Risk Assessment for Perimeter and Access Control Security* and TSA's 2013 through 2015 *Transportation Sector Security Risk Assessments* (TSSRA)—TSA's annual report to Congress on transportation security that establishes risk scores for various attack scenarios within the sector, including domestic aviation. Specifically for vulnerability, in addition to the TSSRAs, we reviewed TSA's use of joint vulnerability assessments (JVA) that TSA conducts with support from the Federal Bureau of Investigation (FBI) at certain airports identified as high risk every 3 years in addition to other airports at their discretion. We analyzed the number and location of JVAs that TSA conducted from fiscal years 2009 through 2015 to report on the extent to which TSA has conducted a system-wide assessment of vulnerability. We selected these timeframes to align with our 2009 report on airport perimeter and access control security and the last full fiscal year of data available at the time of our report.[5] We interviewed TSA officials responsible for risk management activities, including risk assessments, to clarify the extent to which TSA has assessed risk, and its components of threat, vulnerability, and consequence, in relation to airport perimeter and access control security.[6] These agency officials included representatives from the following TSA headquarters offices: Office of Law Enforcement/Federal Air Marshals Service (FAMS), Office of Inspections, Office of Intelligence and Analysis, Office of Security Capabilities, Office of Security Operations, Office of Security Policy and Industry Engagement, and Office of the Chief Risk Officer. We also interviewed officials from the FBI to discuss their role in assessing threat

[5] GAO-09-399.

[6] Threat is a natural or manmade occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property. Vulnerability is a physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard. Consequence is the negative effect of an event, incident, or occurrence.

and vulnerability through the JVA process. We compared information collected through our review of documentation and interviews with agency officials with recommendations on risk assessment and management practices found in the Department of Homeland Security's (DHS) National Infrastructure Protection Plan (NIPP) as well as federal standards for internal controls and our past reports on airport perimeter and access control security.[7]

To determine the extent to which TSA has taken actions since 2009 to oversee and facilitate airport perimeter and access control security, we asked TSA officials to identify agency-led efforts and activities that directly or indirectly impact airport security. For the purposes of this report, we categorized TSA's responses into five main areas of effort: (1) risk planning and assessment, (2) worker security programs, (3) airport security planning and assessment tools, (4) airport guidance and reference materials, and (5) general airport security. To identify the full scope of TSA's oversight of airport security efforts, we interviewed agency officials to identify agency-led efforts and activities that were initiated prior to 2009 and ongoing at the time of our review. Additionally, we interviewed TSA officials responsible for various airport security activities regarding program operations. We also interviewed TSA field officials, airport operator officials, and industry association officials, as described below, regarding selected TSA airport security activities. Further, we interviewed FBI officials regarding the agency's Air Domain Computer Information Comparison program and reviewed relevant documentation.[8] To evaluate TSA efforts with respect to aviation worker security, we reviewed relevant program information for Playbook, *This is*

[7] Department of Homeland Security, *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (2013); Department of Homeland Security, *National Infrastructure Protection Plan Supplemental Tool: Executing a Critical Infrastructure Risk Management Approach* (2013); GAO, *Internal Control: Standards for Internal Controls in the Federal Government*, GAO/AIMD-00.21.3.1 (Washington, D.C.: Nov. 1, 1999); GAO, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls*, GAO-04-728 (Washington, D.C.: June 4, 2004); and GAO-09-399.

[8] The FBI's Air Domain Computer Information Comparison program is a voluntary program that allows airport operators to submit information on aviation workers who have been vetted and received an airport-issued identification credential (badge) for recurring criminal warrants checks.

*My Airport*, and the FBI Rap Back Service program.[9] Additionally, we assessed the extent to which TSA's 2012 *National Strategy for Perimeter and Access Control Security* met NIPP risk management criteria;[10] we also considered the GPRA Modernization Act of 2010 (GPRAMA) requirements, and generally accepted strategic planning practices for government agencies.[11] To assess the extent to which the most recent version of the Strategy has been updated, we compared, among other things, the goals and objectives of the Strategy with activities TSA has initiated since 2009. This included analyzing risk management assessments and relevant program documentation, including budget and performance information. We also interviewed relevant TSA headquarters officials regarding the extent to which the Strategy has been informed by ongoing perimeter and access control security efforts.

To describe the actions selected commercial airports have taken, if any, to strengthen airport perimeter and access control security since 2009, we conducted site visits and telephone interviews with airport officials and onsite TSA federal security directors (FSD) or their representatives at selected airports as well as interviewed industry officials.[12] We conducted site visits at six commercial airports in the United States—Baltimore-Washington International Thurgood Marshall Airport, Chattanooga

[9] TSA defines Playbook as a flexible, risk-based and intelligence-driven deployment system of countermeasures that are coordinated at the local airport level to respond quickly to emergency conditions or hostile acts. *This is My Airport* is a training program for badged airport, tenant, and contractor employees designed to raise security awareness through worker commitments to mission, workplace vigilance, and detection and reporting of suspicious activity at an airport. The FBI Rap Back Service program uses the FBI's fingerprint-based criminal record repository to provide recurrent fingerprint-based criminal history records checks for aviation workers who have been initially vetted and received airport-issued identification credentials.

[10] In 2012, TSA released the *National Strategy for Perimeter and Access Control Security*, which defines how TSA seeks to secure airport perimeters and control access to security-restricted areas of the nation's commercial airports.

[11] Pub. L. No. 111-352, 124 Stat. 3866 (2011). The GPRA Modernization Act of 2010 (GPRAMA) updates the Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285 (1993); GAO, *Agencies' Strategic Plans Under GPRA: Key Questions to Facilitate Congressional Review*, GAO/GGD-10.1.16, Version 1 (Washington, D.C.: May 1997).

[12] FSDs are the ranking TSA authorities responsible for leading and coordinating TSA security activities at the nation's approximately 440 commercial airports.

Metropolitan Airport, Hartsfield-Jackson Atlanta International Airport, Merced Municipal Airport, Monterey Regional Airport, and Norman Y. Mineta San Jose International Airport. During these visits, we observed airport security operations that included various technology- and nontechnology-based approaches intended to strengthen airport security, toured the airports' perimeters, and discussed issues related to perimeter and access control security with onsite FSDs or their representatives, and airport officials. We also conducted telephone interviews with onsite TSA and airport officials from five commercial airports in the United States—Charleston County International Airport and Air Force Base, Dallas-Ft. Worth International Airport, John F. Kennedy International Airport, Logan International Airport, and Miami International Airport. During these interviews, we discussed with officials airport security operations that included airports' approaches intended to strengthen security, unique physical characteristics of the airports, and issues related to perimeter and access control security. We selected these airports for site visits and their officials for telephone interviews based on a variety of factors, including a range in the airport category, public interest as shown through media reports of previous events related to security, unique security characteristics or challenges (such as a water perimeter), and new technology or initiatives implemented by airports related to perimeter and access control security. Because we did not select a generalizable sample of airports, the results of these site visits and interviews cannot be projected to all of the approximately 440 commercial airports in the United States. However, the site visits and interviews provided us with onsite TSA and airport officials' perspectives on actions taken intended to strengthen airport perimeter and access control security, including various approaches using both technology- and nontechnology-based methods. Further, we interviewed officials from the American Association of Airport Executives (AAAE), Airports Council International-North America (ACI-NA), the National Safe Skies Alliance, and RTCA, Inc.'s, Special Committee on Airport Security Access Control Systems. We selected these two industry associations and two specialist non-profit organizations based on input from TSA officials and airport officials, and because of these associations' and organizations' specialized knowledge and experience with airport security operations.[13] These interviews provided us with additional perspectives on airport security.

We conducted this performance audit from February 2015 to May 2016, 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.

[13] According to these two industry associations—American Association of Airport Executives (AAAE) and the Airports Council International-North America (ACI-NA)—their combined membership includes thousands of airport management personnel and represents approximately 95 percent of domestic airline passenger and air cargo traffic in North America, The two non-profit organizations—National Safe Skies Alliance, Inc. ,and RTCA, Inc., a federal aviation advisory committee formerly known as the Radio Technical Commission for Aeronautics—work with airports, government, and the industry to develop related technologies and procedures. RTCA also functions as a federal advisory committee for the review and endorsement of recommendations on a variety of issues—such as technical performance standards—for the FAA.

# Appendix II: Requirements Addressing Security Measures at Commercial Airports

Pursuant to the Aviation and Transportation Security Act (ATSA), as amended, the Transportation Security Administration (TSA) is the federal agency with primary responsibility for ensuring the security of the nation's civil aviation system.[1] Federal regulations governing civil aviation security are primarily codified at Parts 1540 through 1562 of Title 49 of the Code of Federal Regulations (C.F.R.), through which TSA imposes or otherwise enforces security measures and other requirements carried out by airport operators, air carriers, and other civil aviation stakeholders (see tables 4 through 8) as components of the agency's layered approach to security.[2] Airport operators implement security measures relating to perimeter security and access controls primarily in accordance with their respective security programs and any applicable regulations, security directives (SD), or amendments to such security programs, against which TSA also assesses airport operator compliance.[3] This appendix highlights and describes requirements relating to perimeter security and access controls and for which airport operators have primary responsibilities; it does not, however, include all relevant provisions and requirements.[4]

[1] See Pub. L. No. 107-71, 115 Stat. 597 (2001); 49 U.S.C. §§ 114, 44901-46.

[2] For purposes of this appendix, the term "air carrier" encompasses both U.S. aircraft operators and foreign air carriers with security programs or otherwise regulated under 49 C.F.R. parts 1544 or 1546, unless otherwise indicated. For purposes of this appendix, the term "commercial airport" means any airport implementing a TSA-approved security program or otherwise regulated under part 1542.

[3] TSA has designated security directives (SD) and national amendments (NA) to airport security programs (ASP)—formerly referred to as ASP amendments or ASP changes—as Sensitive Security Information (SSI). Therefore, we do not identify or describe specific SDs or NAs in this appendix.

[4] This appendix is not a comprehensive compilation of all requirements addressing security measures at commercial airports. For example, this appendix does not specifically address security measures and other requirements carried out by U.S. or foreign-flagged air carriers that relate to perimeter security and access controls at an airport. It also does not reference, for example, the Airport Security Program (ASP) Guide, which contains recommended best practices for perimeter and access control security, or Information Circulars that, among other things, contain best practices on aviation worker physical inspections, security awareness training and access control.

Table 4: Definitions (49 C.F.R. part 1540)

| Term | Definition |
|---|---|
| **Air Operations Area (AOA)** | A portion of an airport, specified in the airport security program (ASP), in which security measures specified in 49 C.F.R. part 1540 are carried out. The AOA includes aircraft movement areas, aircraft parking areas, loading ramps, and safety areas for use by aircraft operated by air carriers, and any adjacent areas (such as general aviation areas) that are not separated by adequate security systems, measures, or procedures. The AOA does not include the secured area. |
| **Airport operator** | A person who operates an airport serving an air carrier. |
| **Airport security program** | A security program approved by the Transportation Security Administration (TSA) under 49 C.F.R. § 1542.101. |
| **Airport tenant** | Any person, other than an air carrier, that has an agreement with the airport operator to conduct business on airport property. |
| **Airport tenant security program** | An agreement between the airport operator and an airport tenant approved by TSA, that specifies the measures by which the tenant will perform security functions under § 1542.113. |
| **Escort** | To accompany or monitor the activities of an individual who does not have unescorted access authority into or within a secured area or security identification display area (SIDA). |
| **Exclusive area** | Any portion of a secured area, AOA, or SIDA, including individual access points, for which an air carrier has assumed responsibility under § 1542.111. |
| **Exclusive area agreement** | An agreement between the airport operator and an air carrier that permits such an air carrier to assume responsibility for specified security measures in accordance with § 1542.111. |
| **Secured area** | A portion of an airport, specified in the ASP, in which certain security measures specified in part 1542 are carried out. This area is where air carriers enplane and deplane passengers and sort and load baggage and any adjacent areas that are not separated by adequate security measures. |
| **Security identification display area** | A portion of an airport, specified in the ASP, in which security measures specified in part 1540 are carried out. The SIDA includes the secured area and may include other areas of the airport. |
| **Standard security program** | A security program issued by TSA that serves as a baseline for a particular type of operator. If TSA has issued a standard security program for a particular type of operator, unless otherwise authorized by TSA, each operator’s security program consists of the standard security program together with any amendments and alternative procedures approved or accepted by TSA. |
| **Sterile area** | A portion of an airport defined in the ASP that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, or by an air carrier, through the screening of persons and property. |
| **Unescorted access authority** | The authority granted by an airport operator, an air carrier, or an airport tenant, to individuals to gain entry to, and be present without an escort in, secured areas and SIDAs of airports. |

Source: GAO summary of 49 C.F.R. pt. 1540. | GAO-16-632

Table 5: General Provisions (49 C.F.R. part 1542, subpart A)

| Provision | Description |
|---|---|
| Airport Security Coordinator (ASC)<br>(49 C.F.R. § 1542.3) | Each airport operator must designate one or more ASC to, among other things, serve as the airport operator’s primary and immediate contact for security-related activities and communications with the Transportation Security Administration (TSA), review with sufficient frequency all security-related functions to ensure that all are effective and in compliance with part 1542, its security program, and applicable security directives, immediately initiate corrective action for any instance of non-compliance identified through such a review, and review and control the results of employment history, verification, and criminal history records checks required under § 1542.209. |
| Inspection authority<br>(§ 1542.5) | Each airport operator must allow TSA, at any time or place and in accordance with provisions set forth in this section of the regulation, to make any inspections or tests to determine compliance of an airport operator, air carrier, or other airport tenants with 49 C.F.R. chapter XII, subchapter C (49 C.F.R. pts. 1540-62) and any security program under this subchapter, part 1520 of this subchapter (protection of sensitive security information), and 49 U.S.C. Subtitle VII, as amended. At the request of TSA, each airport operator must provide evidence of compliance with part 1542 and its airport security program (ASP). |

Source: GAO summary of 49 C.F.R. pt. 1542, subpt. A. | GAO-16-632

Table 6: Airport Security Program (49 C.F.R. part 1542, subpart B)

| Provision | Description |
|---|---|
| General requirements<br>(§ 1542.101) | An airport security program (ASP) must, among other things, provide for the safety and security of persons and property on an aircraft against an act of criminal violence, aircraft piracy, and the introduction of an unauthorized weapon, explosive, or incendiary device onto an aircraft, be in writing, include applicable items listed in § 1542.103, and be approved by the Transportation Security Administration (TSA). |
| Content<br>(§ 1542.103) | See following information. |

| Except as otherwise approved and in accordance with the regulation, each airport operator must include in its security program: | Complete program[a]<br>§ 1542.103(a) | Supporting program<br>§ 1542.103(b) | Partial program<br>§ 1542.103(c) |
|---|---|---|---|
| Name, means of contact, duties, and training requirement of the Airport Security Coordinator (ASC) (§ 1542.103(a)(1), (b)(1), (c)(1) | X | X | X |
| Description of the secured areas (§ 1542.103(a)(3)) | X | | |
| Description of the Air Operations Area (AOA) (§ 1542.103(a)(4)) | X | | |

| Provision | Description | | | |
|---|---|---|---|---|
| | Description of the security identification display areas (SIDA) (§ 1542.103(5)) | X | | |
| | Description of the sterile areas (§ 1542.103(a)(6)) | X | | |
| | Procedures regarding criminal history record checks<br>(§ 1542.103(a)(7)) | X | | |
| | Description of personnel identification program<br>(§ 1542.103(a)(8)) | X | | |
| | Escort procedures<br>(§ 1542.103(a)(9)) | X | | |
| | Challenge procedures<br>(§ 1542.103(a)(10)) | X | | |
| | Training programs<br>(§ 1542.103(a)(11), (b)(3), (c)(3)) | X | X | X |
| | Description of law enforcement support<br>(§ 1542.103(a)(12), (b)(2), (c)(2)) | X | X | X |
| | System for maintaining records<br>(§ 1542.103(a)(13), (b)(4), (c)(4)) | X | X | X |
| | Procedures and description of facilities and equipment used to support TSA inspection of individuals and property, and air carrier screening functions (§ 1542.103(a)(14)) | X | | |
| | Contingency plan<br>(§ 1542.103(a)(15), (b)(5)) | X | X | |
| | Procedures for distribution, storage, and disposal of security programs, directives, Information Circulars, implementing instructions, and, as appropriate, classified information<br>(§ 1542.103(a)(16), (b)(6), (c)(5)) | X | X | X |
| | Procedures for posting public advisories<br>(§ 1542.103(a)(17), (b)(7), (c)(6)) | X | X | X |
| | Incident management procedures (§ 1542.103(a)(18), (b)(8), (c)(7)) | X | X | X |

| Provision | Description | |
|---|---|---|
| | **Alternate security procedures, if any, that the airport operator intends to use in the event of natural disasters, and other emergency or unusual conditions (§ 1542.103(a)(19))** | X |
| | **Each exclusive area agreement**<br>**(§ 1542.103(a)(20))** | X |
| | **Each airport tenant security program (§ 1542.103(a)(21))** | X |
| **Approval and amendments**<br>**(§ 1542.105)** | Each airport operator required to have a security program under part 1542 must submit its proposed program to the designated TSA official for approval in the manner prescribed in this section of the regulation (§ 1542.105(a)). Except as otherwise specified in the regulation, an airport operator may, as prescribed in the regulation, submit a request to the designated TSA official to amend its security program (§ 1542.105(b)). If safety and the public interest require an amendment, the designated TSA official may undertake to amend a security program as prescribed in the regulation (§ 1542.105(c)). The designated TSA official may, upon finding that there is an emergency requiring immediate action with respect to safety and security in air transportation or in air commerce and in the manner prescribed in the regulation, issue an amendment effective on the date of receipt by the airport operator (§ 1542.105(d)). | |
| **Changed conditions affecting security**<br>**(§ 1542.107)** | After approval of a security program, an airport operator must, in accordance with the regulation, notify TSA of changes to measures, training, area descriptions, or staffing described in the security program, in air carrier operations that would require modifications to the security program, or to the layout or physical structure of the airport used to support required screening process, access, presence or movement control functions. The airport operator must inform TSA of each interim measure being taken to maintain adequate security until an appropriate security program is approved, and each interim measure must be acceptable to TSA. | |
| **Alternate means of compliance**<br>**(§ 1542.109)** | If in TSA's judgment the overall safety and security of the airport and air carrier operations are not diminished, TSA may approve a security program that provides for the use of alternative measures. Such a program may be considered only for an airport operator at which service by an air carrier is determined by TSA to be seasonal or infrequent. | |
| **Exclusive area agreements**<br>**(§ 1542.111)** | TSA may approve an amendment to an ASP under which an air carrier assumes responsibility for specified security measures for all or portions of the secured area, AOA, or SIDA, including access points, provided the assumption of responsibility is exclusive to an air carrier (i.e., responsibility may not be shared among air carriers). | |
| **Airport tenant security programs**<br>**(§ 1542.113)** | Under a TSA-approved airport tenant security program, for which TSA must find that the tenant is able and willing to carry out the security program, the tenant must assume responsibility for specified security measures of the secured area, AOA, or SIDA; may not assume responsibility for law enforcement support under § 1542.215; must assume responsibility within the tenant's leased areas or areas designated for the tenant's exclusive use but may not assume responsibility for the airport passenger terminal; and have exclusive responsibility (i.e., responsibility may not be shared among tenants). | |

Source: GAO summary of 49 C.F.R. pt. 1542, subpt. B. | GAO-16-632

[a] Although the regulation sets out the specific criteria that will determine the type of security program an airport operator must implement, in general, Transportation Security Administration (TSA)-regulated (i.e., commercial) airports in Categories X through III must implement complete security programs. TSA classifies the nation's approximately 440 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 largest number of passenger boardings and Category IV airports have the smallest.

Table 7: Operations (49 C.F.R. part 1542, subpart C)

| Provision | Description |
|---|---|
| **Secured area**<br>**(§ 1542.201)** | Each airport operator required to have a complete security program must establish at least one secured area and must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into and within the secured area in accordance with the regulation (see below). |
| **Air Operations Area (AOA)**<br>**(§ 1542.203)** | Each airport operator required to have a complete security program must establish an AOA, unless the entire area is designated as a secured area, and must prevent and detect the unauthorized entry, presence, and movement of individuals and ground vehicles into or within the AOA in accordance with the regulation (see below). |
| **Security identification display area (SIDA)**<br>**(§ 1542.205)** | Each airport operator required to have a complete security program must establish, in accordance with the regulation, at least one SIDA and must establish and carry out measures to prevent the unauthorized presence and movement of individuals in the SIDA in accordance with the regulation (see below). |

| The airport operator must: | Secured area (§ 1542.201)[a] | AOA (§ 1542.203)[b] | SIDA (§ 1542.205)[c] |
|---|---|---|---|
| **Establish and carry out measures for controlling entry in accordance with § 1542.207.** | X | X | X |
| **Provide for detection of, and response to, each unauthorized presence or movement, or attempted entry, by an individual whose access is not authorized in accordance with its security program.** | X | X | X |
| **Establish and carry out a personnel identification system described under § 1542.211.** | X | | X |
| **Subject each individual to employment history verification as described in § 1542.209 (i.e., a fingerprint-based criminal history records check) before authorizing unescorted access.** | X | | X |
| **Train each individual before granting unescorted access, as required in § 1542.213(b).** | X | | X |
| **Provide security information as described in § 1542.213(c) to each individual with unescorted access.** | | X | |

| Provision | Description | | | |
|---|---|---|---|---|
| | **Post signs at access points and on the perimeter that provide warning of the prohibition against unauthorized entry.** | X | X | X |
| **Access control systems**<br>**(§ 1542.207)** | Unless the Transportation Security Administration (TSA) approves an amendment to a security program that provides alternative measures that provide an overall equal level of security, measures for controlling entry to the secured area must ensure that only those individuals authorized to have unescorted access to the secured area are able to gain entry, ensure that an individual is immediately denied entry to a secured area when that person's access authority to the area is withdrawn, and provide a means to differentiate between individuals authorized to have access to an entire secured are and individuals authorized access to only a particular portion of a secured area (§ 1542.207(a)-(b)). Measures for controlling entry to the AOA must incorporate accountability procedures to maintain their integrity (§ 1542.207(c)). An airport operator may issue a second access medium to an individual who has unescorted access to a secured areas or the AOA, but is temporarily not in possession of the original access medium, in accordance with provisions set forth in the regulation (§1542.207(d)). | | | |
| **Fingerprint-Based criminal history records checks**<br>**(§ 1542. 209)** | In accordance with provisions set forth in the regulation, an airport operator may generally not grant unescorted access authority to an individual unless the individual has undergone a fingerprint-based criminal history records check that does not disclose that he or she has a disqualifying criminal offense (§ 1542.209(b)). An individual has a disqualifying criminal offense if he or she has been convicted, or found not guilty by reason of insanity, of any of the crimes listed in the regulation 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 (§ 1542.209(d)). Among other provisions, if information becomes available to the airport operator indicating that an individual with unescorted access authority has a disqualifying criminal offense, the airport operator must determine the status of the conviction and if confirmed immediately revoke any unescorted access authority (§ 1542.209(l)(3)).[d] | | | |
| **Identification systems**<br>**(§ 1542.211)** | Requirements on the airport operator for, among other things, the content and display of, and accountability for personnel identification media, for the use of temporary identification media, and for the establishment and implementation of challenge and escort procedures.[e] | | | |
| **Training**<br>**(§ 1542.213)** | Requirements on the airport operator, in accordance with the regulation, to ensure that individuals performing security functions for the airport operator and individuals with unescorted access to the secured area, SIDA, and AOA are trained or briefed on the provisions of part 1542, security directives, Information Circulars, and the security program, to the extent that such individuals need to know in order to perform their duties. | | | |
| **Law enforcement-related requirements**<br>**(§§ 1542.215-1542.221)** | Requirements on the airport operator pertaining to the presence of law enforcement support (§ 1542.215), qualifications and training of law enforcement personnel (§ 1542.217), the availability of supplemental law enforcement personnel (§ 1542.219), and the maintenance of records concerning law enforcement action (§ 1542.221). | | | |

Source: GAO summary of 49 C.F.R. pt. 1542, subpt. C. | GAO-16-632

[a] Each secured area must be a security identification display area (SIDA). § 1542.205(a)(1).

[b] If approved by TSA, an airport operator may designate all or portions of its Air Operations Area (AOA) as a SIDA or, in accordance with the regulation, use another personnel identification system, as part of its means for meeting its requirements. §1542.203(b)(5).

[c] The regulation specifies the portions of an AOA and the areas of an airport, in addition to the secured area, that must be a SIDA. § 1542.205(a).

[d] An airport operator may accept the certification of an aircraft operator regulated under part 1544 indicating that it has complied with § 1544.229 (fingerprint-based criminal history records check applicable) for the aircraft operator's employees and contractors seeking unescorted access authority. § 1542.209(n).

[e] For example, personnel identification media must convey a full-face image, full name, employer, and identification number of the individual to whom the identification medium is issued; indicate clearly the scope of the individual's access and movement privileges; indicate clearly an expiration date; and be of sufficient size and appearance to be readily observable for challenge purposes. § 1542.211(a)(1).

Table 8: Contingency Measures (49 C.F.R. part 1542, subpart D)

| Provision | Description |
|---|---|
| **Contingency plan**<br>**(§ 1542.301)** | Each airport operator with a complete or supporting program must adopt a contingency plan and implement its plan when directed by the Transportation Security Administration (TSA), conduct reviews and exercises of its plan, and ensure that all parties involved know their responsibilities and that all information contained in the plan is current. TSA may approve alternative implementation measures, reviews, and exercises to the contingency plan which will provide an overall level of security equal to the required contingency plan. |
| **Security directives and Information Circulars**<br>**(§ 1542.303)** | TSA may issue an Information Circular to notify airport operators of security concerns and may issue a security directive (SD) setting forth mandatory measures if it determines that additional security measures are necessary to respond to a threat assessment or to a specific threat against civil aviation. Among other things, airport operators must comply with SDs within the time prescribed in the directive, and submit proposed alternative measures to TSA for approval if unable to implement the measures in a S D. Each airport operator that receives a SD or Information Circular and each person who receives information from a SD or Information Circular must restrict the availability of, and refuse to release, such information except as permitted in § 1542.303(f). |
| **Public advisories**<br>**(§ 1542.305)** | When advised by TSA, each airport operator must, in accordance with their security program, prominently display and maintain in public areas information concerning foreign airports that, in the judgment of the Secretary of Transportation, do not maintain and administer effective security measures.[a] |
| **Incident management**<br>**(§ 1542.307)** | Except as otherwise specified in the regulation, each airport operator must establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations. In general, airport operators must, at least once every 12 calendar months, review the procedures established pursuant to this section with all persons having responsibilities for such procedures to ensure that all parties know their responsibilities and that all procedures are current. |

Source: GAO summary of 49 C.F.R. pt. 1542, subpt. D. | GAO-16-632

[a] The regulation, as presently codified, does not reflect the transfer of aviation security responsibilities from the Federal Aviation Administration (FAA) to the Transportation Security Administration (TSA) within the Department of Transportation pursuant to the Aviation and Transportation Security Act (ATSA) and the subsequent transfer of TSA from the Department of Transportation to the Department of Homeland Security (DHS) pursuant to the Homeland Security Act of 2002. As such, it is the TSA Administrator, by delegation of authority from the Secretary of Homeland Security, who determines whether a foreign airport maintains and administers effective security measures."

# Appendix III: Ongoing Efforts Initiated Prior to 2009 to Regulate and Facilitate Airport Perimeter and Access Control Security

The Transportation Security Administration (TSA) has numerous ongoing activities that were initiated prior to 2009, which either directly or indirectly regulate, strengthen, or facilitate commercial airport perimeter and access control security. A list of these ongoing efforts—as identified by TSA officials—is presented in Table 9. TSA officials cited agency policy recommendations and requirements—such as security directives—and compliance inspections as playing a particularly important role in regulating and facilitating perimeter and access control security at commercial airports, as well as the following general transportation security program that addresses airport perimeter and access control:

- **Visible Intermodal Prevention and Response (VIPR) program.** According to TSA officials, the agency implemented the VIPR program in 2005 to protect the nation's transportation systems through targeted deployment of integrated TSA assets. VIPR teams utilize screening and law enforcement capabilities in coordinated activities to randomly and unpredictably augment security across all modes of transportation, including the aviation sector. VIPR teams are composed of TSA officials—including Federal Air Marshals, transportation security inspectors, behavior detection officers, and explosives specialists—and local law enforcement and airport officials. These teams provide law enforcement and screening capabilities, including randomly screening aviation workers, property, and vehicles, as well as providing a visible presence at access points and the security-restricted areas of airports. According to TSA, during fiscal year 2015, TSA's 31 VIPR teams conducted approximately 7,250 operations nationwide in the aviation environment. In response to the November 2013 shooting at the Los Angeles International Airport, in which a TSA screener was killed, TSA redeployed VIPR teams to the aviation sector, to establish a baseline 60/40 split of VIPR resources between the aviation and surface transportation sectors.[1] TSA officials stated that, as of December 2015, the agency had maintained this increased VIPR presence at commercial airports.

[1] On November 1, 2013, an individual entered terminal 3 at Los Angeles International Airport and shot and killed a TSA screener and wounded two other TSA screeners and a passenger. According to TSA officials, the actual percentage of Visible Intermodal Prevention and Response (VIPR) resources applied to aviation and surface transportation sectors ranged from 57 to 64 percent on a monthly basis between November 2014 and December 2015, due to VIPR responses to short-term, risk-driven issues and the requests of transportation stakeholders.

Table 9: Additional Ongoing Airport Perimeter and Access Control Security-Related Actions the Transportation Security Administration (TSA) Initiated Prior to 2009

| Type of security action | Action | Description |
|---|---|---|
| Risk assessment | Joint Vulnerability Assessments (JVA) – since TSA inception[a] | JVAs are assessments that teams of TSA special agents and other officials conduct jointly with the Federal Bureau of Investigation (FBI) every 3 years for airports identified as high risk. |
| Airport guidance and reference materials | Recommended Security Guidelines for Airport Planning, Design and Construction – last revised 2011 | Developed by TSA and aviation security stakeholders, the recommended guidelines intend to bring an airport-wide focus to the various planning and design issues surrounding airside, landside, terminal perimeter, information technology, surveillance, access control, and the publicly accessible side of the airport. The guidance contains no legal or regulatory mandates. |
| General airport security | Annual airport compliance inspections – since TSA inception[a] | The Aviation and Transportation Security Act (ATSA) directed TSA to, on an ongoing basis, test airport operators for compliance with access control requirements, report annually on the findings of the assessments, assess the effectiveness of penalties in ensuring compliance with security procedures, and take any other appropriate enforcement actions when noncompliance is found.[b] According to TSA, the agency also routinely performs comprehensive, targeted, and supplemental inspections and other compliance activities, such as assessments, investigations, tests, and audits of airport identification media/badges, among other things. TSA also reviews compliance with airport security program (ASP) requirements and amendments. |
| | Law Enforcement Officer Reimbursement Program[c] – 2002 | The Law Enforcement Officer Reimbursement Program was established to provide partial reimbursement for law enforcement presence in support of the passenger screening checkpoint. In June 2003, the program was expanded so officers may also patrol airport perimeters, be stationed at airport access points to assist with worker and passenger screening, or both. |
| | Security directives/national amendments – since TSA inception[a] | TSA may issue security directives that impose additional requirements on airport operators if it determines that such measures are needed to respond to general or specific threats against the civil aviation system. TSA may also require airport operators to adopt national amendments to their ASPs if it determines such measures are needed. |
| | Standard Operating Procedures (SOP) – since TSA inception[a] | TSA identifies aviation worker screening requirements through various SOPs, such as the Known Crew Member and Screening Checkpoint SOPs. |
| | Behavior Detection and Analysis Program (formerly known as Screening of Passengers by Observation Techniques (SPOT) Program) – 2003 | Piloted in 2003 and 2004 and incrementally expanded as a nationwide program starting in fiscal year 2007, SPOT is a screening program in which behavior detection officers are to identify individuals who may pose a security threat to aviation security through the observation of behavioral indicators. |
| | Insider Threat Assessments – since TSA inception[a] | TSA periodically conducts assessments of the insider threat at selected airports. |

Source: GAO analysis of TSA information. | GAO-16-632

Notes: This table does not include Transportation Security Administration (TSA) airport security programs and activities that we reported on in 2009 and which, according to TSA officials, have been closed out or are no longer in active use. These include the Aviation Credential Interoperability Solution, a standardized credentialing program; technology pilot programs; the Airport Access Control Pilot Program and the Airport Perimeter Security pilot project, designed to provide information on new and emerging technologies and commercially available technology; and the Worker Screening Pilot test, a worker screening pilot program designed to assess various methods for screening airport workers before they enter secured areas.

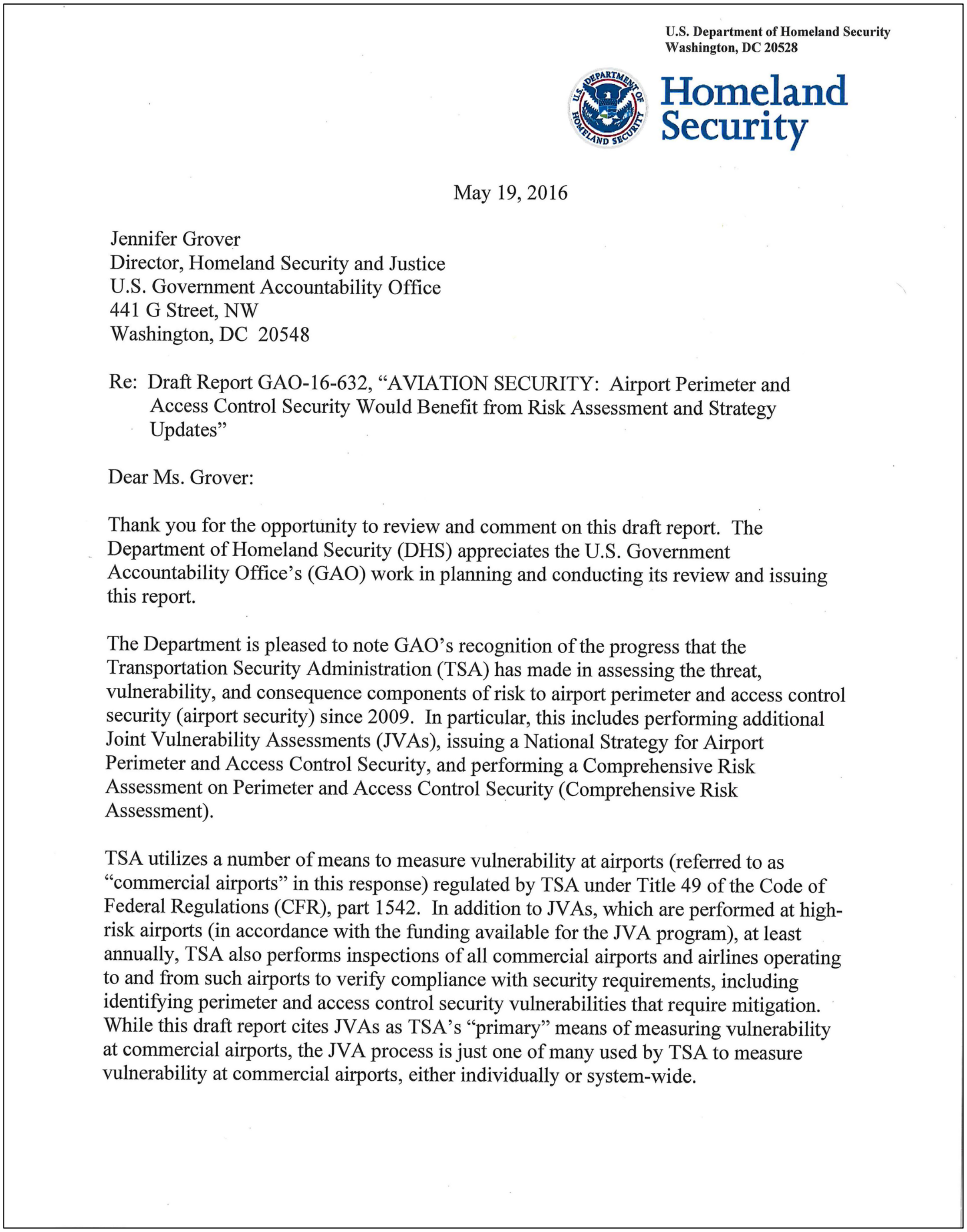
This table also does not include programs or activities by federal agencies other than TSA that address or indirectly support airport perimeter and access control security. Examples include the Federal Bureau of Investigation (FBI) Air Domain Computer Information Comparison Initiative, a recurring criminal warrants check for airport workers who have received airport-issued identification credentials, or grants awarded by the Federal Aviation Administration (FAA) to commercial airports through the Airport Improvement Program. The FBI's Air Domain Computer Information Comparison Initiative program is a voluntary program that allows airport operators to submit information on aviation workers who have been vetted and received an airport-issued identification credential (badge) for recurring criminal warrants checks. According to the FBI, this program specifically addresses the vulnerability that badged individuals within the airport environment seldom receive routine criminal warrants checks after their initial employment background check.

[a] These activities were also performed under the FAA, prior to the establishment of TSA. See, e.g., Air Transportation Security Act of 1974, Pub. L. No. 93-366, tit. II, § 315, 88 Stat. 409, 415-418 (1974) (directing the Administrator of the FAA to prescribe or continue in effect reasonable regulations relating to screening of passengers, air transportation security, among other responsibilities). Specifically, FAA special agents performed aviation security inspections and the agency issued security bulletins and security directives.

[b] See 49 U.S.C. § 44903(g)(2)(D).

[c] Pursuant to 49 U.S.C. § 44903(c) and 49 C.F.R. § 1542.215, a commercial airport must maintain a law enforcement presence and capability at the airport in the number and manner adequate to support its security program and other security functions at the airport. According to TSA officials, as part of the Law Enforcement Officer Reimbursement Program, a reimbursable cooperative agreement is negotiated between TSA and the respective airport operator to reimburse the operator for funds expended on law enforcement efforts per the terms of the cooperative agreement. See 49 C.F.R. § 1542.219.

# Appendix IV: Comments from the Department of Homeland Security (DHS)



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

Homeland
Security

May 19, 2016

Jennifer Grover
Director, Homeland Security and Justice
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

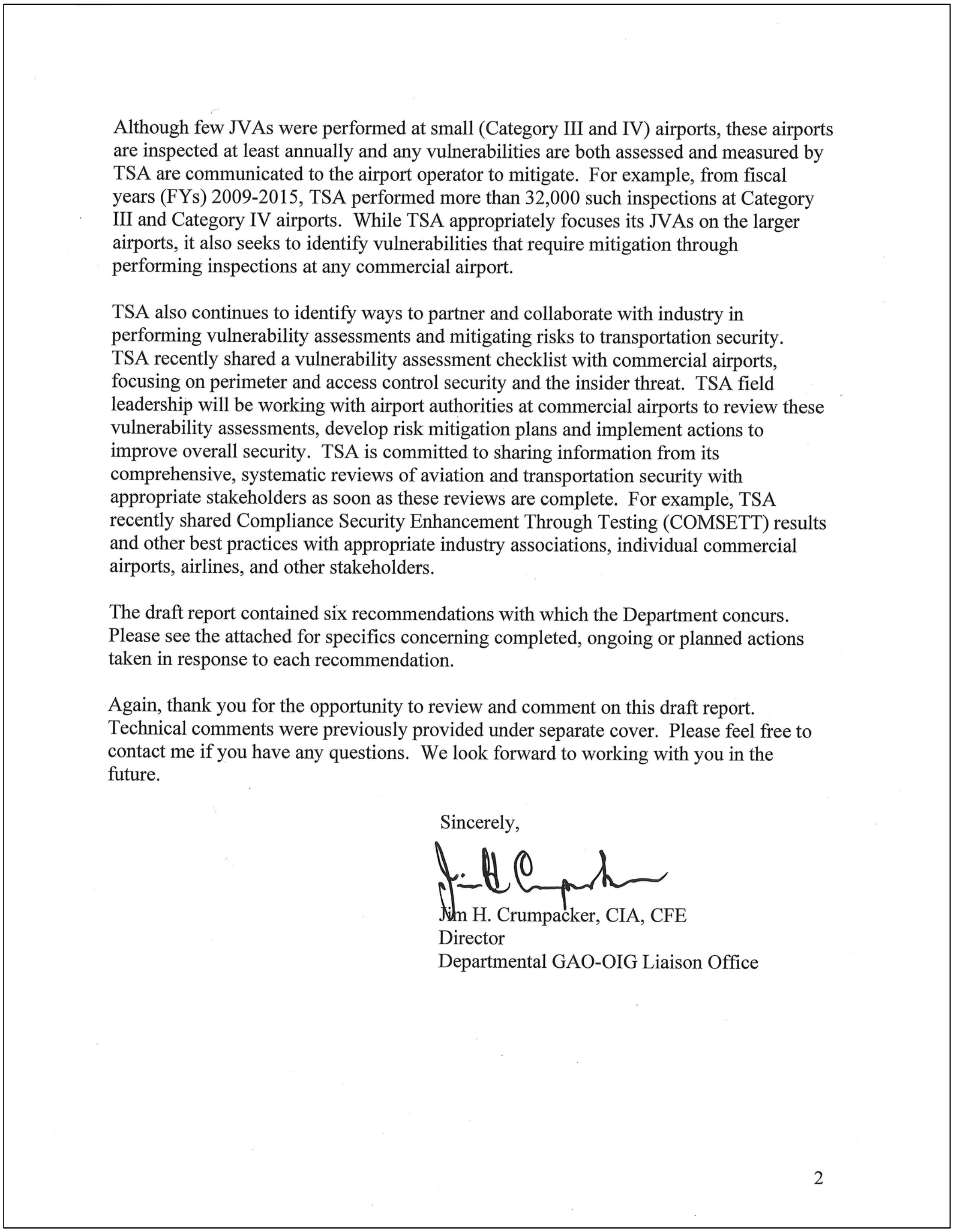
Re: Draft Report GAO-16-632, "AVIATION SECURITY: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates"

Dear Ms. Grover:

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

The Department is pleased to note GAO's recognition of the progress that the Transportation Security Administration (TSA) has made in assessing the threat, vulnerability, and consequence components of risk to airport perimeter and access control security (airport security) since 2009. In particular, this includes performing additional Joint Vulnerability Assessments (JVAs), issuing a National Strategy for Airport Perimeter and Access Control Security, and performing a Comprehensive Risk Assessment on Perimeter and Access Control Security (Comprehensive Risk Assessment).

TSA utilizes a number of means to measure vulnerability at airports (referred to as "commercial airports" in this response) regulated by TSA under Title 49 of the Code of Federal Regulations (CFR), part 1542. In addition to JVAs, which are performed at high-risk airports (in accordance with the funding available for the JVA program), at least annually, TSA also performs inspections of all commercial airports and airlines operating to and from such airports to verify compliance with security requirements, including identifying perimeter and access control security vulnerabilities that require mitigation. While this draft report cites JVAs as TSA's "primary" means of measuring vulnerability at commercial airports, the JVA process is just one of many used by TSA to measure vulnerability at commercial airports, either individually or system-wide.



Although few JVAs were performed at small (Category III and IV) airports, these airports are inspected at least annually and any vulnerabilities are both assessed and measured by TSA are communicated to the airport operator to mitigate. For example, from fiscal years (FYs) 2009-2015, TSA performed more than 32,000 such inspections at Category III and Category IV airports. While TSA appropriately focuses its JVAs on the larger airports, it also seeks to identify vulnerabilities that require mitigation through performing inspections at any commercial airport.

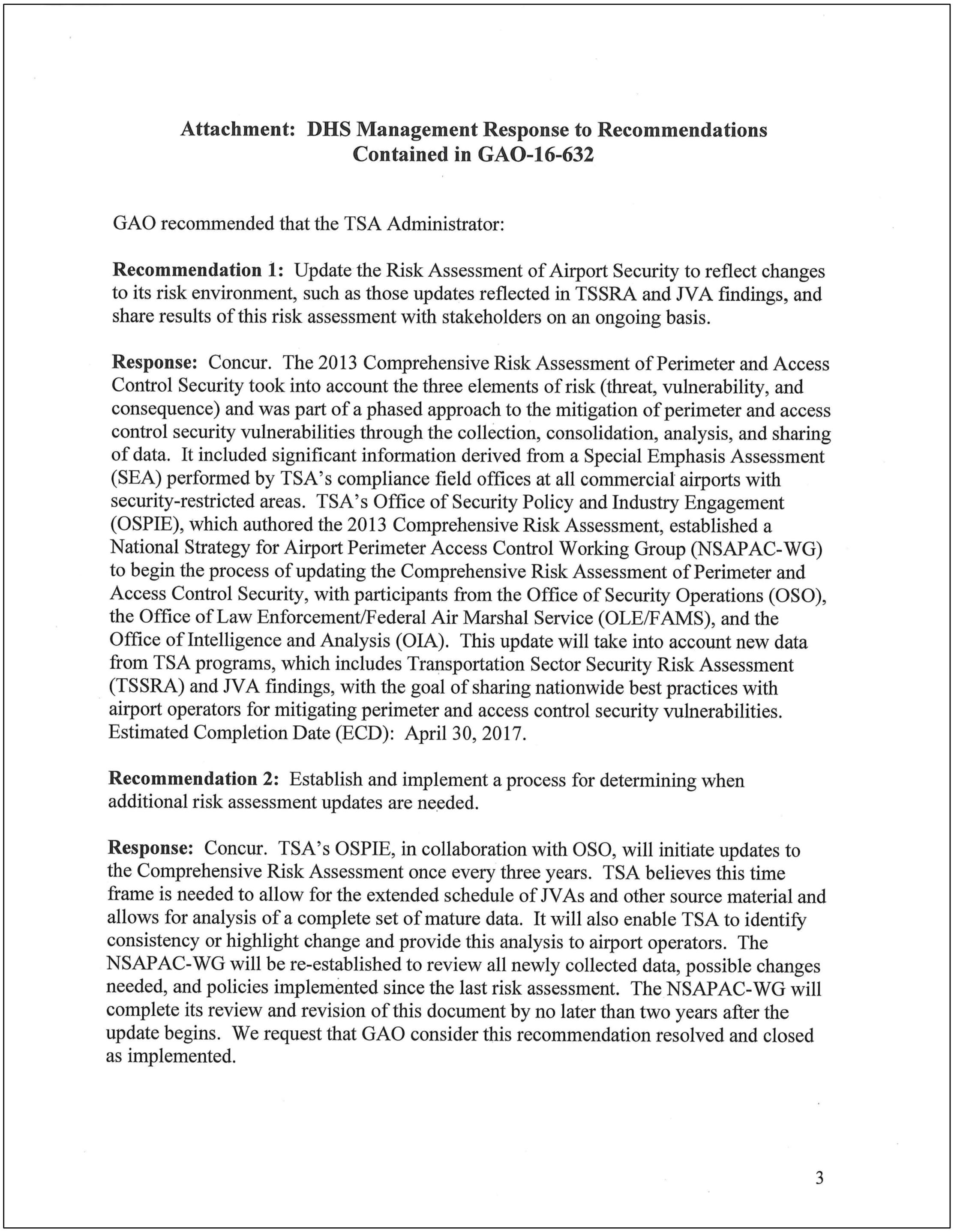
TSA also continues to identify ways to partner and collaborate with industry in performing vulnerability assessments and mitigating risks to transportation security. TSA recently shared a vulnerability assessment checklist with commercial airports, focusing on perimeter and access control security and the insider threat. TSA field leadership will be working with airport authorities at commercial airports to review these vulnerability assessments, develop risk mitigation plans and implement actions to improve overall security. TSA is committed to sharing information from its comprehensive, systematic reviews of aviation and transportation security with appropriate stakeholders as soon as these reviews are complete. For example, TSA recently shared Compliance Security Enhancement Through Testing (COMSETT) results and other best practices with appropriate industry associations, individual commercial airports, airlines, and other stakeholders.

The draft report contained six recommendations with which the Department concurs. Please see the attached for specifics concerning completed, ongoing or planned actions taken in response to each recommendation.

Again, thank you for the opportunity to review and comment on this draft report. Technical comments were previously provided under separate cover. Please feel free to contact me if you have any questions. We look forward to working with you in the future.

Sincerely,

Jim H. Crumpacker, CIA, CFE<br>
Director<br>
Departmental GAO-OIG Liaison Office



## Attachment: DHS Management Response to Recommendations Contained in GAO-16-632

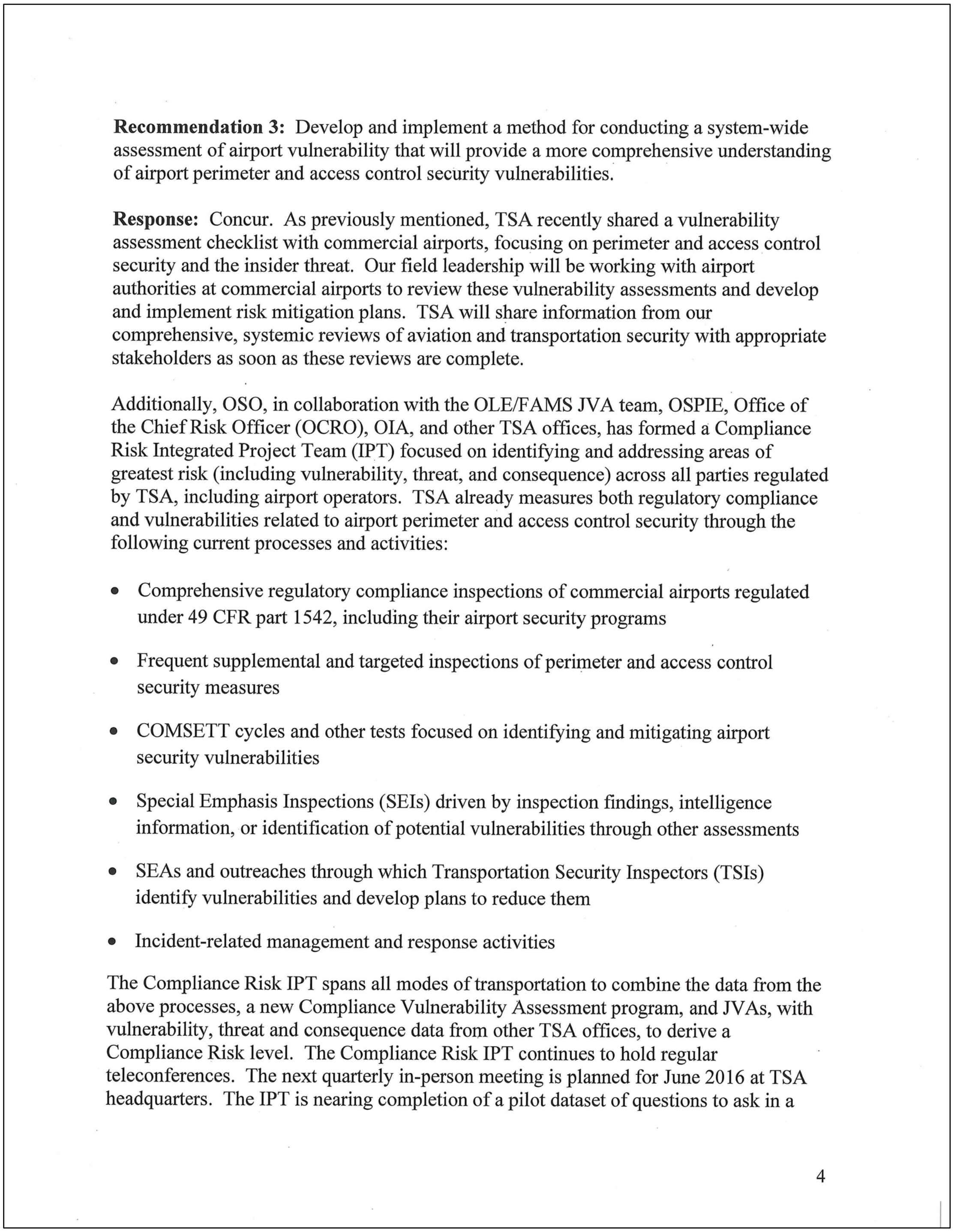
GAO recommended that the TSA Administrator:

**Recommendation 1:** Update the Risk Assessment of Airport Security to reflect changes to its risk environment, such as those updates reflected in TSSRA and JVA findings, and share results of this risk assessment with stakeholders on an ongoing basis.

**Response:** Concur. The 2013 Comprehensive Risk Assessment of Perimeter and Access Control Security took into account the three elements of risk (threat, vulnerability, and consequence) and was part of a phased approach to the mitigation of perimeter and access control security vulnerabilities through the collection, consolidation, analysis, and sharing of data. It included significant information derived from a Special Emphasis Assessment (SEA) performed by TSA's compliance field offices at all commercial airports with security-restricted areas. TSA's Office of Security Policy and Industry Engagement (OSPIE), which authored the 2013 Comprehensive Risk Assessment, established a National Strategy for Airport Perimeter Access Control Working Group (NSAPAC-WG) to begin the process of updating the Comprehensive Risk Assessment of Perimeter and Access Control Security, with participants from the Office of Security Operations (OSO), the Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS), and the Office of Intelligence and Analysis (OIA). This update will take into account new data from TSA programs, which includes Transportation Sector Security Risk Assessment (TSSRA) and JVA findings, with the goal of sharing nationwide best practices with airport operators for mitigating perimeter and access control security vulnerabilities. Estimated Completion Date (ECD): April 30, 2017.

**Recommendation 2:** Establish and implement a process for determining when additional risk assessment updates are needed.

**Response:** Concur. TSA's OSPIE, in collaboration with OSO, will initiate updates to the Comprehensive Risk Assessment once every three years. TSA believes this time frame is needed to allow for the extended schedule of JVAs and other source material and allows for analysis of a complete set of mature data. It will also enable TSA to identify consistency or highlight change and provide this analysis to airport operators. The NSAPAC-WG will be re-established to review all newly collected data, possible changes needed, and policies implemented since the last risk assessment. The NSAPAC-WG will complete its review and revision of this document by no later than two years after the update begins. We request that GAO consider this recommendation resolved and closed as implemented.



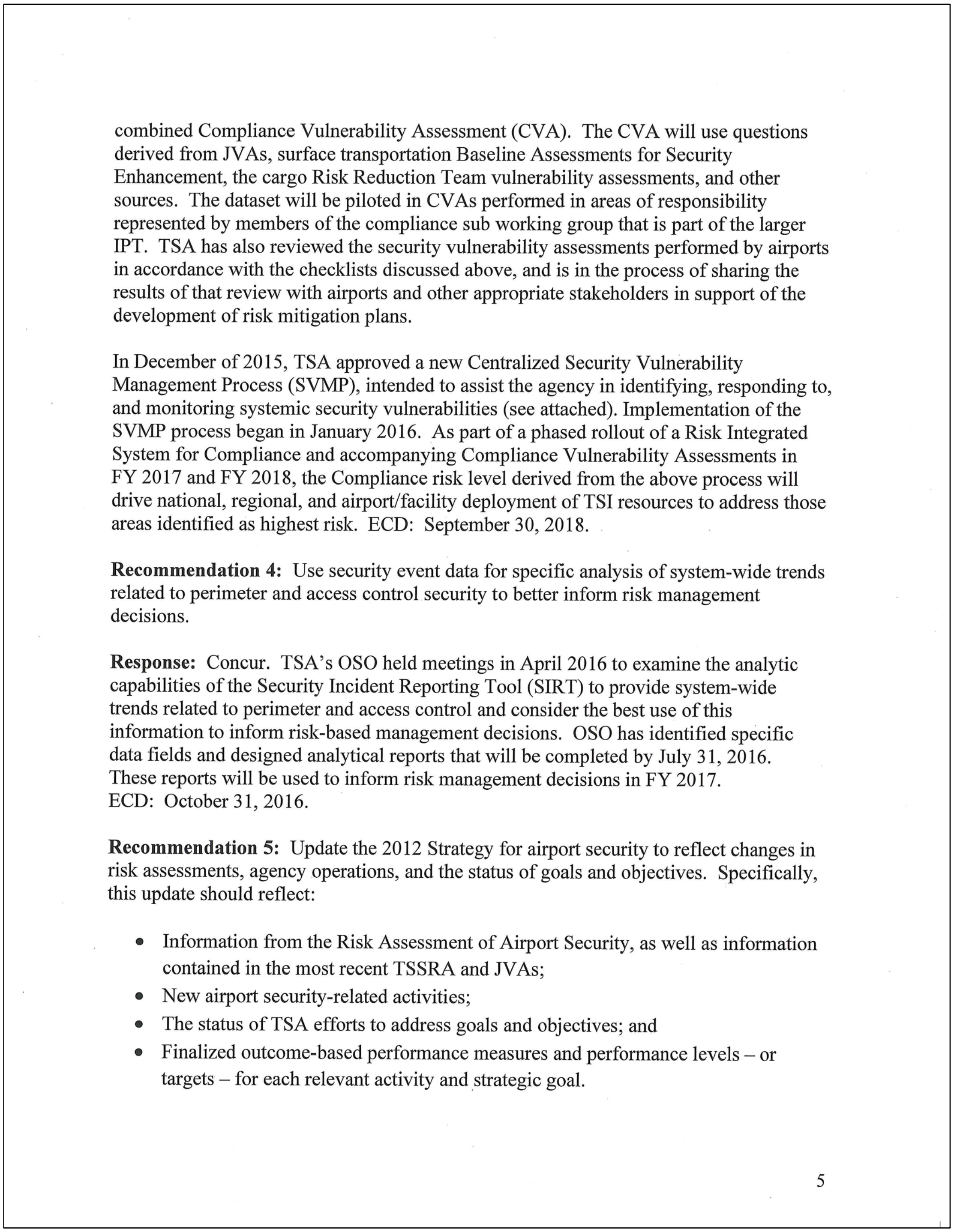
**Recommendation 3:** Develop and implement a method for conducting a system-wide assessment of airport vulnerability that will provide a more comprehensive understanding of airport perimeter and access control security vulnerabilities.

**Response:** Concur. As previously mentioned, TSA recently shared a vulnerability assessment checklist with commercial airports, focusing on perimeter and access control security and the insider threat. Our field leadership will be working with airport authorities at commercial airports to review these vulnerability assessments and develop and implement risk mitigation plans. TSA will share information from our comprehensive, systemic reviews of aviation and transportation security with appropriate stakeholders as soon as these reviews are complete.

Additionally, OSO, in collaboration with the OLE/FAMS JVA team, OSPIE, Office of the Chief Risk Officer (OCRO), OIA, and other TSA offices, has formed a Compliance Risk Integrated Project Team (IPT) focused on identifying and addressing areas of greatest risk (including vulnerability, threat, and consequence) across all parties regulated by TSA, including airport operators. TSA already measures both regulatory compliance and vulnerabilities related to airport perimeter and access control security through the following current processes and activities:

- Comprehensive regulatory compliance inspections of commercial airports regulated under 49 CFR part 1542, including their airport security programs
- Frequent supplemental and targeted inspections of perimeter and access control security measures
- COMSETT cycles and other tests focused on identifying and mitigating airport security vulnerabilities
- Special Emphasis Inspections (SEIs) driven by inspection findings, intelligence information, or identification of potential vulnerabilities through other assessments
- SEAs and outreaches through which Transportation Security Inspectors (TSIs) identify vulnerabilities and develop plans to reduce them
- Incident-related management and response activities

The Compliance Risk IPT spans all modes of transportation to combine the data from the above processes, a new Compliance Vulnerability Assessment program, and JVAs, with vulnerability, threat and consequence data from other TSA offices, to derive a Compliance Risk level. The Compliance Risk IPT continues to hold regular teleconferences. The next quarterly in-person meeting is planned for June 2016 at TSA headquarters. The IPT is nearing completion of a pilot dataset of questions to ask in a



combined Compliance Vulnerability Assessment (CVA). The CVA will use questions derived from JVAs, surface transportation Baseline Assessments for Security Enhancement, the cargo Risk Reduction Team vulnerability assessments, and other sources. The dataset will be piloted in CVAs performed in areas of responsibility represented by members of the compliance sub working group that is part of the larger IPT. TSA has also reviewed the security vulnerability assessments performed by airports in accordance with the checklists discussed above, and is in the process of sharing the results of that review with airports and other appropriate stakeholders in support of the development of risk mitigation plans.

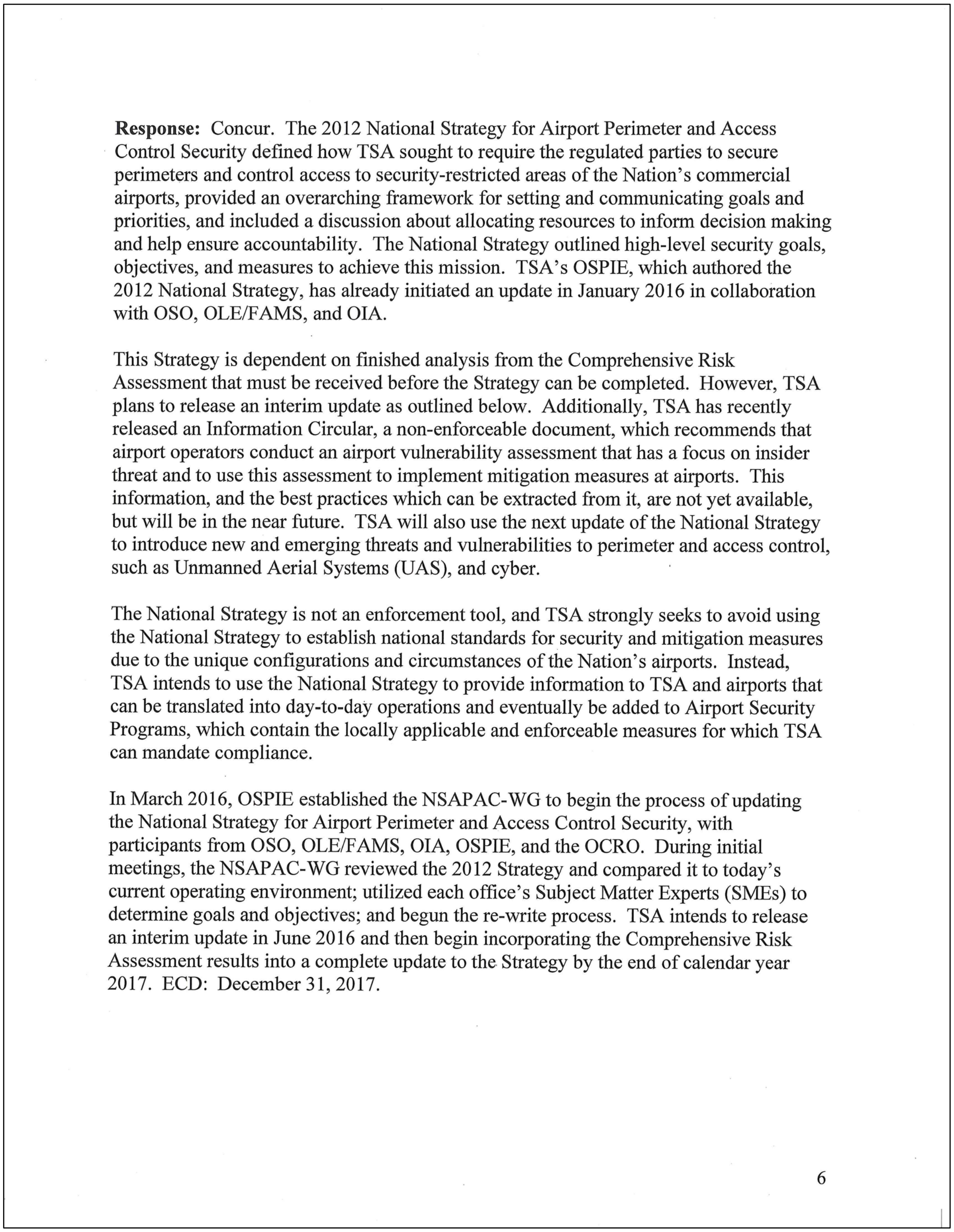
In December of 2015, TSA approved a new Centralized Security Vulnerability Management Process (SVMP), intended to assist the agency in identifying, responding to, and monitoring systemic security vulnerabilities (see attached). Implementation of the SVMP process began in January 2016. As part of a phased rollout of a Risk Integrated System for Compliance and accompanying Compliance Vulnerability Assessments in FY 2017 and FY 2018, the Compliance risk level derived from the above process will drive national, regional, and airport/facility deployment of TSI resources to address those areas identified as highest risk. ECD: September 30, 2018.

**Recommendation 4:** Use security event data for specific analysis of system-wide trends related to perimeter and access control security to better inform risk management decisions.

**Response:** Concur. TSA's OSO held meetings in April 2016 to examine the analytic capabilities of the Security Incident Reporting Tool (SIRT) to provide system-wide trends related to perimeter and access control and consider the best use of this information to inform risk-based management decisions. OSO has identified specific data fields and designed analytical reports that will be completed by July 31, 2016. These reports will be used to inform risk management decisions in FY 2017.
ECD: October 31, 2016.

**Recommendation 5:** Update the 2012 Strategy for airport security to reflect changes in risk assessments, agency operations, and the status of goals and objectives. Specifically, this update should reflect:

- Information from the Risk Assessment of Airport Security, as well as information contained in the most recent TSSRA and JVAs;
- New airport security-related activities;
- The status of TSA efforts to address goals and objectives; and
- Finalized outcome-based performance measures and performance levels – or targets – for each relevant activity and strategic goal.

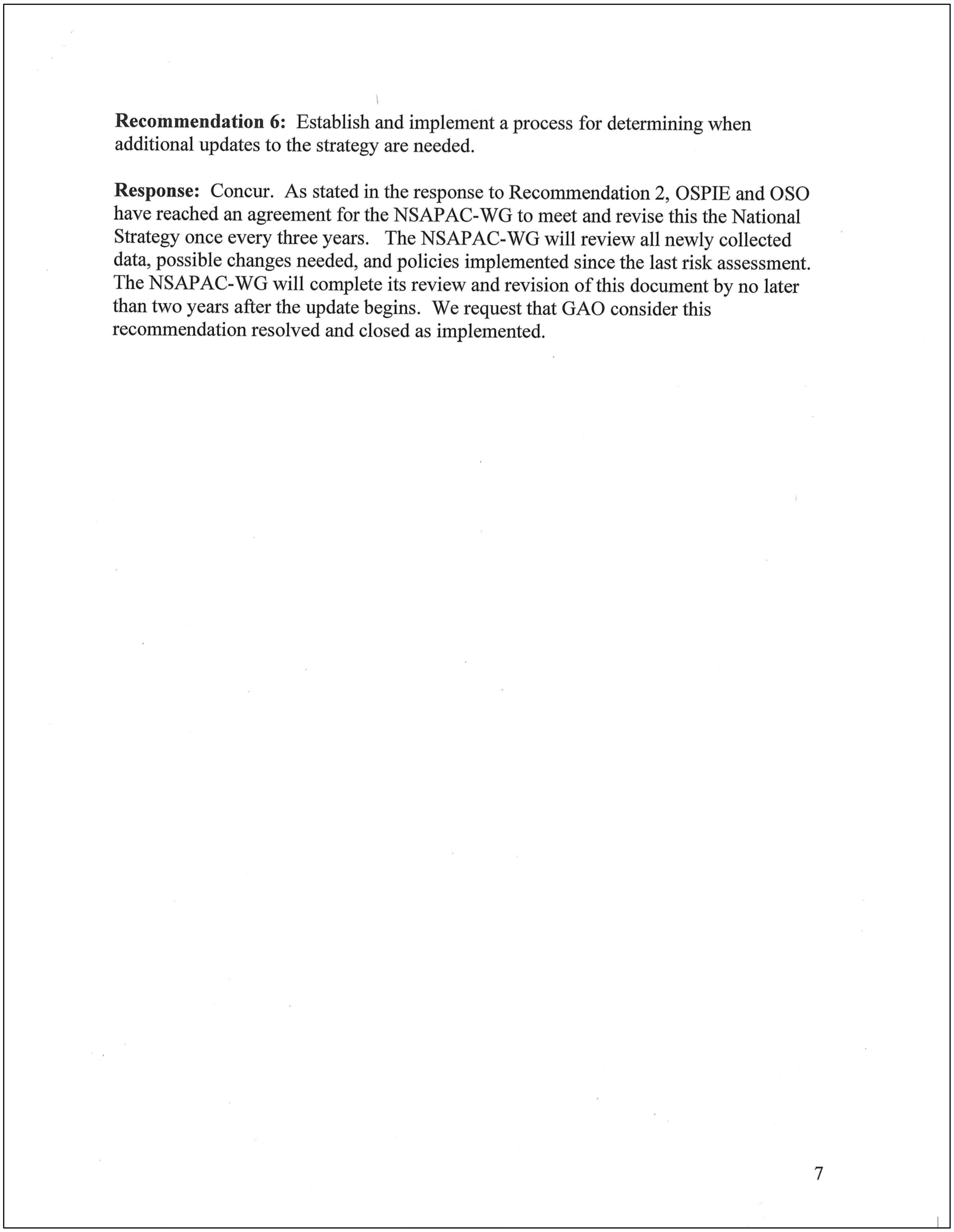


**Response:** Concur. The 2012 National Strategy for Airport Perimeter and Access Control Security defined how TSA sought to require the regulated parties to secure perimeters and control access to security-restricted areas of the Nation's commercial airports, provided an overarching framework for setting and communicating goals and priorities, and included a discussion about allocating resources to inform decision making and help ensure accountability. The National Strategy outlined high-level security goals, objectives, and measures to achieve this mission. TSA's OSPIE, which authored the 2012 National Strategy, has already initiated an update in January 2016 in collaboration with OSO, OLE/FAMS, and OIA.

This Strategy is dependent on finished analysis from the Comprehensive Risk Assessment that must be received before the Strategy can be completed. However, TSA plans to release an interim update as outlined below. Additionally, TSA has recently released an Information Circular, a non-enforceable document, which recommends that airport operators conduct an airport vulnerability assessment that has a focus on insider threat and to use this assessment to implement mitigation measures at airports. This information, and the best practices which can be extracted from it, are not yet available, but will be in the near future. TSA will also use the next update of the National Strategy to introduce new and emerging threats and vulnerabilities to perimeter and access control, such as Unmanned Aerial Systems (UAS), and cyber.

The National Strategy is not an enforcement tool, and TSA strongly seeks to avoid using the National Strategy to establish national standards for security and mitigation measures due to the unique configurations and circumstances of the Nation's airports. Instead, TSA intends to use the National Strategy to provide information to TSA and airports that can be translated into day-to-day operations and eventually be added to Airport Security Programs, which contain the locally applicable and enforceable measures for which TSA can mandate compliance.

In March 2016, OSPIE established the NSAPAC-WG to begin the process of updating the National Strategy for Airport Perimeter and Access Control Security, with participants from OSO, OLE/FAMS, OIA, OSPIE, and the OCRO. During initial meetings, the NSAPAC-WG reviewed the 2012 Strategy and compared it to today's current operating environment; utilized each office's Subject Matter Experts (SMEs) to determine goals and objectives; and begun the re-write process. TSA intends to release an interim update in June 2016 and then begin incorporating the Comprehensive Risk Assessment results into a complete update to the Strategy by the end of calendar year 2017. ECD: December 31, 2017.



**Recommendation 6:** Establish and implement a process for determining when additional updates to the strategy are needed.

**Response:** Concur. As stated in the response to Recommendation 2, OSPIE and OSO have reached an agreement for the NSAPAC-WG to meet and revise this the National Strategy once every three years. The NSAPAC-WG will review all newly collected data, possible changes needed, and policies implemented since the last risk assessment. The NSAPAC-WG will complete its review and revision of this document by no later than two years after the update begins. We request that GAO consider this recommendation resolved and closed as implemented.

# Appendix V: GAO Contact and Staff Acknowledgments

## GAO Contact

Jennifer Grover (202) 512-7141 or groverj@gao.gov

## Acknowledgments

In addition to the contact named above, Christopher E. Ferencik (Assistant Director), Barbara A. Guffy (Analyst-in-Charge), Ana Ivelisse Aviles, Chuck Bausell, Katherine M. Davis, Michele C. Fejfar, Eric D. Hauswirth, Susan Hsu, Thomas F. Lombardi, Elizabeth D. Luke, Ruben Montes de Oca, Faye R. Morrison, Heidi J. Nielson, and Maria C. Staunton made key contributions to this report.

(100785)

## 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 GAO's website (http://www.gao.gov). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to http://www.gao.gov and select "E-mail Updates."

### 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, http://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 E-mail Updates.
Listen to our Podcasts and read The Watchblog.
Visit GAO on the web at www.gao.gov.

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: http://www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@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