United States Government Accountability Office

Report to Congressional Committees

September 2017

AVIATION SECURITY

TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016

Accessible Version

GAO-17-662

September 2017

AVIATION SECURITY

TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016

GAO Highlights

Highlights of GAO-17-662, a report to congressional committees

Why GAO Did This Study

Recent incidents involving aviation workers conducting criminal activity in the nation's commercial airports have led to interest in the measures TSA and airport operators use to control access to secure areas of airports. The 2016 ASA required TSA to take several actions related to oversight of access control security at airports. The Act also contains a provision for GAO to report on progress made by TSA.

This report examines, among other issues, progress TSA has made in addressing the applicable requirements of the 2016 ASA. GAO compared information obtained from TSA policies, reports, and interviews with TSA officials to the requirements in the 2016 ASA. GAO also visited three airports to observe their use of access controls and interviewed TSA personnel. The non-generalizable group of airports was selected to reflect different types of access control measures and airport categories.

GAO is not making any recommendations. In its formal response, DHS stated that it continues to implement the 2016 ASA requirements.

View GAO-17-662. For more information, contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov

What GAO Found

The Transportation Security Administration (TSA) has generally made progress addressing the 69 applicable requirements within the Aviation Security Act of 2016 (2016 ASA). As of June 2017, TSA had implemented 48 of the requirements; it plans no further action on these. For 18 requirements, TSA officials took initial actions and plans further action. TSA officials stated they have yet to take action on 2 requirements and plan to address them in the near future. TSA officials took no action on 1 requirement regarding access control rules because it plans to address this through mechanisms other than formal rulemaking, such as drafting a national amendment to airport operator security programs. Key examples of TSA's progress in implementing the requirements in the eight relevant sections of the Act are shown below:

Conduct a Threat Assessment: TSA conducted a threat assessment that analyzed vulnerabilities related to the insider threat—that is, the threat posed by aviation workers who exploit their access privileges to secure areas of an airport for personal gain or to inflict damage.

Enhance Oversight Activities: Among other things, TSA developed a list of measures for airport operators to perform, such as an airport rebadging if the percent of badges unaccounted for exceeds a certain threshold.

Update Airport Employee Credential Guidance: TSA issued guidance to airport operators to match the expiration date of a non-U.S. citizen aviation worker's identification badge to the individual's U.S. work authorization status.

Vet Airport Employees: In addition to making progress on updating employee vetting rules, TSA coordinated with the Federal Bureau of Investigation (FBI) to implement the FBI's Rap Back service for providing recurrent fingerprint-based criminal history record checks for aviation workers.

Develop and Implement Access Control Metrics: TSA developed and implemented a metric that determines the percentage of TSA secure area inspections found to be in compliance with the airport security program.

Develop a Tool for Unescorted Access Security: According to TSA officials, they developed a tool designed to ensure that aviation workers with unescorted access are randomly screened for prohibited items, such as firearms and explosives, and to check for proper identification.

Increase Covert Testing: TSA plans to increase the number of covert tests of access controls it will perform in 2017.

Review Security Directives: Security directives are issued by TSA when, for example, additional measures are required to respond to a threat. TSA officials stated they review all security directives annually to consider the need for revocation or revision, and brief Congress when new directives are to be issued.

Contents

Tables

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

September 7, 2017

Congressional Committees:

The Transportation Security Administration (TSA) and the Federal Bureau of Investigation (FBI) consider one of aviation security's most pressing concerns to be the insider threat—the threat of aviation workers who exploit their access privileges to secure areas of an airport for personal gain or to inflict damage.[1] Recent incidents involving aviation workers conducting criminal activity in the nation's commercial airports have led to congressional concern about access controls, the measures TSA and commercial airport operators use to manage access to secure areas.[2] For example, in December 2014, a baggage handler at Atlanta, Georgia's Hartsfield-Jackson International Airport was arrested for allegedly using his airport-issued identification badge to repeatedly smuggle loaded and unloaded firearms into the passenger boarding area for hand-off to an accomplice, who carried the firearms onto airplanes bound for New York.[3] In June 2015, a man pleaded guilty for a 2013 incident in which he attempted to use his airport identification badge credentials to access the

[1]A "secure area of an airport" is the sterile area and the Secure Identification Display Area (SIDA) of an airport (as such terms are defined in 49 C.F.R. § 1540.5). See Pub. L. No. 114-190, § 3402(a)(1), 130 Stat. 615, 656 (2016) (citing 49 U.S.C. § 44903(j)(2)(H)). See also 49 C.F.R. § 1540.5 (providing that the secured area, SIDA (referred to as the Security Identification Display Area in the regulation), and sterile area, as those terms are defined in the regulation, and other areas of the airport for which access is controlled will be specified in the respective airport's security program).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.

[2]A "commercial airport" is an airport in the United States operating under a TSA-approved security program in accordance with 49 C.F.R. part 1542 that, in general, regularly serves air carriers with scheduled passenger operations (also referred to as "TSA-regulated airports"). Access controls include the security features that control access to the secure areas of an airport, and includes identification badges. See, e.g., 49 C.F.R. § 1542.211 (establishing requirements for airport operators' personnel identification system). For purposes of this report, an "aviation worker" is an employee, contractor, or representative of an airport, domestic or foreign airline, vendor, concessionaire, tenant, government agency, entity in the air cargo supply chain, or other entity working or operating at an airport.

[3]For purposes of this report, the term "identification badge" refers to credentials used by aviation workers to gain unescorted access to a secure area of a commercial airport.

tarmac at the Wichita, Kansas Mid-Continent Airport with the intent of exploding a car bomb.

As the federal agency with primary responsibility for securing the nation's civil aviation system, TSA, within the Department of Homeland Security (DHS), is responsible for establishing minimum security measures and regulating the implementation of those measures by airport operators and other regulated entities to improve access control security. As part of this responsibility, TSA conducts inspections and covert testing to maintain and improve access controls that reduce security risks posed by aviation workers. Among other things, TSA may 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.[4]

In 2016, we reported that TSA had made progress since 2009 in assessing the risk to airport perimeter and access control security by developing its *Comprehensive Risk Assessment of Perimeter and Access Control Security* in May 2013.[5] However, we also reported that TSA had not updated this assessment to reflect changes in the airport security risk environment, including risks from insider threats. We recommended that TSA update this assessment to reflect these changes, and take other actions related to airport security. DHS concurred with the recommendation and in June 2017 TSA officials stated that actions were underway to implement the recommendation. The Department of Homeland Security's Office of Inspector General has also recently reported on TSA's challenges in managing access control security, including the need for additional oversight over identification badges.[6]

Enacted on July 15, 2016, Subtitle D of the Aviation Security Act of 2016 (ASA) requires TSA to take specific actions in eight categories related to aviation worker screening and access control security: (1) conduct a

[4]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).

[5]GAO, *Aviation Security: Airport Perimeter and Access Control Security Would Benefit from Risk Assessment and Strategy Updates,* GAO-16-632 (Washington D.C.: May 31, 2016).

[6]Department of Homeland Security, Office of Inspector General, *TSA Could Improve Its Oversight of Airport Controls Over Access Media Badges,* OIG-17-04 (Washington D.C.: October 14, 2016).

threat assessment, (2) enhance oversight activities, (3) update airport employee credential guidance, (4) vet airport employees, (5) develop and implement access control metrics, (6) develop a tool for unescorted access security, (7) increase covert testing, and (8) review security directives.[7] The Act also contains a provision for GAO to report on progress made by TSA and the effect on aviation security of implementing the applicable 2016 ASA requirements.[8] This report examines (1) progress TSA has made in addressing the applicable requirements of the 2016 ASA and (2) the potential effects on aviation security TSA has identified in implementing these requirements.

To determine the progress TSA has made in addressing the applicable requirements of the 2016 ASA, we examined relevant TSA policies and procedures, including applicable regulations and security directives, and reports that TSA was required to submit to the appropriate congressional committees in accordance with applicable provisions of the 2016 ASA—including those in draft form—and compared them to the applicable 2016 ASA requirements.[9] We interviewed TSA officials responsible for implementing each of the applicable 2016 ASA requirements, including officials from the Office of Security Policy and Industry Engagement, the Office of Chief Counsel, the Office of Intelligence and Analysis, and the Office of Security Operations to determine what actions they had taken, and plan to take, in response to the applicable 2016 ASA requirements. For the purposes of this report, we define progress as TSA having taken action on a requirement or having a commitment for planned actions.

To determine the potential effects on aviation security TSA has identified in implementing these requirements, we interviewed TSA officials responsible for implementing the 2016 ASA requirements to gain their insight on which requirements they believed may have an impact on aviation security, and subsequently reviewed relevant documents, including those in draft form. Because many of TSA's actions taken in response to the 2016 ASA were recently implemented or are still ongoing

[7]Pub. L. No. 114-190, tit. III, subtit. D, 130 Stat. 615, 656-62 (2016) (enacted as part of the Title III of the FAA Extension, Safety, and Security Act of 2016).

[8]§ 3410, 130 Stat. at 662.

[9]The Act provides that "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

and not fully implemented, we did not assess the effectiveness of the actions taken by TSA.

We conducted site visits to Dulles International Airport, Virginia, and Dallas Fort Worth International Airport and Dallas Love Field, Texas. During these visits, we observed these airports' use of access controls—such as aviation worker use of identification badges to gain access to the secure areas—in their operations and discussed these controls with airport officials and TSA federal security directors or their representatives. We selected these airports for site visits and interviews based on the variation in the types of access controls these airports implemented and the different airport categories.[10] 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 the perspectives of TSA personnel and airport officials on how actions taken by TSA to implement the applicable requirements of the 2016 ASA may affect aviation security.

We conducted this performance audit from February 2017 to September 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[10]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. Dulles International Airport and Dallas Fort Worth International Airport are classified as category X airports. Dallas Love Field Airport is classified as a category I airport.

Background

TSA inspects airports, air carriers, and other regulated entities to ensure that they are in compliance with federal aviation security regulations, TSA-approved airport security programs, and other requirements, including requirements related to controlling airport employee access to secure areas of an airport.[11] Airport operators have direct responsibility for implementing security requirements in accordance with their TSA-approved airport security programs. In general, secure areas of an airport are specified in the airport operator's security programs and include the sterile area, which is the area of an airport that provides passengers access to boarding aircraft and to which access is generally controlled by TSA or a private screening entity under TSA oversight, and the security identification display area (SIDA), which is a portion of an airport in which security measures are carried out and where appropriate identification must be worn by aviation workers.[12] For example, aviation workers that require access to the aircraft movement and parking areas for the purposes of their employment duties must display appropriate identification to access these areas.

Airport operators are to perform background checks on individuals prior to granting them unescorted access to secure areas of an airport and TSA relies on airport operators to collect and verify applicant data, such as name, place of birth, and country of citizenship, for individuals seeking credentials.[13] Background checks for individuals applying for credentials to allow unescorted access to secure areas of commercial airports include (1) a security threat assessment from TSA, including a terrorism check; (2) a fingerprint-based criminal history records check; and (3) evidence that the applicant is authorized to work in the United States. The criminal history records check also determines whether the applicant has committed a disqualifying criminal offense in the previous ten years.

[11]See generally 49 C.F.R. pt. 1542.

[12]See Pub. L. No. 114-190, § 3402(a)(1), 130 Stat. at 656 (citing 49 U.S.C. § 44903(j)(2)(H), which defines "secure area of an airport"); see also 49 C.F.R. § 1540.5.

[13]See 49 C.F.R. §§ 1542.207-1542.211 and TSA Security Directive 1542-04-08L, December 23, 2016. Security Directive 1542-04-08L provides an exception for criminal history records check for Federal, State, or local employees who already have criminal history records check performed as conditions of their employment.

TSA and airport operators have oversight responsibilities for the identification badges that are issued. For example, airport operators must account for all badges through control procedures, such as audits, specified in TSA's security directives and in an airport's security program.[14] TSA assesses airports' compliance with its security directives and federal regulations through inspections conducted in alternating years of, among other things, the airport operator's documents related to issuing and controlling identification badges and by randomly screening aviation workers.

TSA Generally Made Progress in Addressing the Applicable Requirements of the Aviation Security Act of 2016

The Transportation Security Administration (TSA) has generally made progress addressing the 69 applicable requirements within the Aviation Security Act of 2016 (2016 ASA). As of June 2017, TSA officials stated it had implemented 48 of the requirements; it plans no further action on these. For 18 requirements, TSA officials took initial actions and plans further action. TSA officials stated they have yet to take action on 2 requirements and plan to address them in the near future. TSA officials took no action on 1 requirement regarding access control rules because it plans to address this through mechanisms other than formal rulemaking, such as drafting a national amendment to airport operator security programs. Appendix I presents the details of each requirement, the progress made by TSA, and the status of TSA's plans for further actions. A summary of TSA's progress in implementing the requirements in each section of the Act is presented below.[15]

[14]Security Directive 1542-04-08L, Attachment B, I.B.1. TSA's security directive requires airport operators to, among other things, complete a comprehensive audit of all airport-issued access media badges at least once every year to verify the employment and operational need for an identification badge for all badge holders. If more than 5 percent of all airport-issued, unexpired identification badges for any nonpublic area are lost, stolen, or otherwise unaccounted for, the airport operator must reissue identification badges for that nonpublic area.

[15]Each of the categories represents a specific section of the 2016 ASA. See §§ 3402-09, 130 Stat. at 656-62. Each section of the 2016 ASA has multiple requirements for TSA to implement. For more information on the specific requirements in each category, see Appendix I.

Conduct a Threat Assessment (Section 3402)

TSA made progress on the 11 requirements in Section 3402 of the 2016 ASA. TSA plans no further action for 9 requirements and plans further action for 2 requirements, as shown in appendix I. For example, section 3402(a) requires TSA to conduct a threat assessment that considers the seven factors stated in the law and 3402(b) requires TSA to submit a report to the appropriate congressional committees on the results of the assessment.[16] Consistent with these sections, TSA conducted a threat assessment on the level of risk individuals with unescorted access to the secure area of an airport pose to the domestic air transportation system and submitted a report on it to the appropriate congressional committees in May 2017. In conducting the threat assessment, TSA also considered all seven required factors. For example, TSA considered recent security breaches at domestic and foreign airports by analyzing access-control related incidents from December 2013 through February 2017. TSA also considered the vulnerabilities associated with unescorted access authority granted to foreign airport operators and air carriers, and their workers, by reviewing the vulnerability of incoming flights to the United States for four international regions. The threat assessment noted several recommendations under consideration, such as enhancing relationships with the FBI and U.S. Drug Enforcement Administration, among other law enforcement entities, to ensure TSA is more fully aware of insider threats within the domestic transportation system. TSA officials stated they plan to use the threat assessment to, among other things, expand the use of vulnerability assessments and insider threat-related inspections at all commercial airports. Thus, TSA plans no further action for the 9 requirements related to the threat assessment.[17]

[16]The seven factors TSA was required to consider are: (1) domestic intelligence, (2) international intelligence, (3) the vulnerabilities associated with unescorted access authority granted to domestic airport operators and air carriers, and their workers, (4) the vulnerabilities associated with unescorted access authority granted to foreign airport operators and air carriers, and their workers, (5) the processes and practices designed to mitigate the vulnerabilities associated with unescorted access privileges granted to airport operators and air carriers, and their workers; (6) the recent security breaches at domestic and foreign airports, and (7) the recent security improvements at domestic airports, including the implementation of recommendations made by relevant advisory committees, including the Aviation Security Advisory Committee. § 3402(a)(2), 130 Stat. at 656. The report to the committees is also to include any recommendations for improving aviation security. § 3402(b)(1), 130 Stat. at 657.

[17]TSA plans further actions to address the requirements at sections 3402(b)(2) and (3).

Enhance Oversight Activities (Section 3403)

TSA generally made progress in addressing the 10 requirements in Section 3403 of the 2016 ASA. Of the 10 requirements, TSA plans no further action for 4 requirements. TSA plans further action for 5 requirements, but has yet to begin implementing 1 of these 5 requirements. In addition, TSA took no action on one requirement because they plan to address this requirement through other means, as shown in appendix I. Section 3403(a) requires TSA to update rules on access controls, and as part of this update, to consider, among other things best practices for airport operators that report missing more than three percent of credentials for unescorted access to the SIDA of any airport.[18] In accordance with this requirement, TSA developed a list of measures for airport operators to perform—such as an airport rebadging if the percent of unaccounted for badges exceeds a certain threshold—and published them on DHS's Homeland Security Information Network (HSIN) for airport operators to access.[19] In addition, TSA officials stated they developed a fine structure for non-category X airport operators that have more than five percent and for category X airports that have more than three percent of credentials missing for unescorted access to the SIDA of an airport. TSA plans to take additional action to address this and other requirements related to updating the rules on access controls. For example, it plans to propose a national amendment to airport operator

[18]The Act requires TSA to consider the following: (1) increased fines and advanced oversight for airport operators that report missing more than five percent of credentials for unescorted access to any SIDA of an airport; (2) best practices for category X airport operators that report missing more than three percent of credentials for unescorted access to any SIDA of an airport; (3) additional audits and status checks for airport operators that report missing more than three percent of credentials for unescorted access to any SIDA of an airport; (4) review and analysis of the prior five years of audits for airport operators that report missing more than three percent of credentials for unescorted access to any SIDA of an airport; (5) increased fines and direct enforcement requirements for both airport workers and their employers that fail to report within 24 hours an employment termination or a missing credential for unescorted access to any SIDA of an airport; and (6) a method for termination by the employer of any airport worker who fails to report in a timely manner missing credentials for unescorted access to any SIDA of an airport. § 3403(a)(2), 130 Stat. at 657.

[19]The HSIN is a secure web portal that federal, state, local, international, and private sector homeland security partners use to share Controlled Unclassified Information, analyze data, and send alerts.

security programs for airport operators to report to TSA when an airport exceeds a specified threshold for unaccounted identification badges.[20]

TSA plans no further action under section 3403(a)(2)(F) to consider a method of termination by the employer of any airport worker who fails to report in a timely manner missing credentials for unescorted access to any SIDA of an airport. TSA officials stated they considered developing such a method; however, they plan no further action because TSA does not have authority over employment determinations made by airport operators or other employers.[21] Further, section 3403(b) stated that TSA may encourage the issuance of temporary credentials by airports and aircraft operators of free one-time, 24-hour temporary credentials for aviation workers who report their credentials as missing but not permanently lost. Officials stated they plan no further action on this requirement because temporary credentials conflict with a current federal regulation that requires airport operators to ensure that only one identification badge is issued to an individual at one time.[22]

TSA has yet to take action on one requirement and took no action on another requirement in section 3403(a) of the 2016 ASA. First, TSA stated they plan to consider section 3403(a)(2)(E) to increase fines and direct enforcement action for airport workers and their employers who fail to timely report missing credentials, but have yet to do so. In addition, TSA took no action to update the rules on access controls. TSA officials stated that that they are taking other actions, such as drafting a proposed national amendment to airport security programs, to address this requirement.

[20]As of July 2017, TSA's proposed national amendments are in draft form. In accordance with 49 C.F.R. § 1542.105, a national amendment proposed by TSA requires (1) notice to airport operators, in writing, of the proposed amendment while allowing not less than 30 days for the airport operator to provide comment on the amendment; (2) TSA consideration of relevant materials, including comment provided by airport operators; and (3) notification by TSA to airport operators of the adoption or rescission of the amendment.

[21]TSA officials further stated that while TSA has authority to prohibit the issuance of an identification badge, it does not have authority over airport operators' or other employers' personnel practices.

[22]See 49 C.F.R. § 1542.211(a)(3)(vi).

Update Airport Employee Credential Guidance (Section 3404)

TSA generally made progress in addressing the 4 requirements in Section 3404 of the 2016 ASA. Of the 4 requirements, TSA took action and plans no further action for 2 requirements, plans further actions for 1 requirement, and has yet to take action on 1 requirement. For example, section 3404(a) requires TSA to issue guidance to airport operators regarding the placement of an expiration date on airport identification badges issued to non-U.S. citizens that is not longer than the period of time during which such non-U.S. citizens are lawfully authorized to work in the United States. In accordance with this requirement, TSA issued guidance that states that airport operators should match an identification badge's expiration date to an individual's immigration status, published this guidance to airport operators in fiscal year 2016 on the HSIN, and plans to issue a security directive to further address this requirement.[23] TSA has no plans for further action to address section 3404(b)(1), which requires TSA to issue guidance for its inspectors to annually review the procedures of airport operators and carriers for individuals seeking unescorted access to the SIDA and to make information on identifying suspicious or fraudulent identification materials available to airport operators and air carriers. For example, TSA officials stated that Transportation Security Inspector guidance is updated yearly to incorporate additional inspection guidelines, as is TSA's Compliance Manual, which includes updated methods for inspections and additional airport access control measures to be tested. The update for fiscal year 2017 changed the number of required tests related to insider threats and has new inspection techniques related to individuals seeking unescorted access to the SIDA. Additionally, officials stated that TSA made information available on the HSIN on identifying fraudulent documentation.

TSA officials have yet to take action on section 3404(b)(2), which requires that the guidance to airport operators regarding the placement of an expiration date on airport identification badges issued to non-U.S. citizens include a comprehensive review background checks and employment authorization documents issues by the United States Citizenship and Immigration Services. Officials stated that it plans to request clarification from the appropriate congressional committees to determine the actions needed to implement this requirement.

[23]As of July 2017, TSA's security directive to address this requirement is in draft form.

Vet Airport Employees (Section 3405)

TSA made progress on the 12 requirements in Section 3405 of the 2016 ASA. TSA plans no further action for 5 requirements, and plans further action for 7 requirements, as shown in appendix I. For example, section 3405(a) requires TSA to revise certain regulations related to the eligibility requirements and disqualifying criminal offenses for individuals seeking unescorted access to any SIDA of an airport. In accordance with this requirement, TSA is drafting a Notice of Proposed Rulemaking to update rules related to vetting of employees seeking unescorted access to the SIDA of an airport; however, TSA officials reported two challenges in implementation. First, TSA officials stated they cannot update the employee eligibility requirements and disqualifying criminal offense regulations within the required 180 days specified in the statute because the required process for promulgating regulations generally takes longer than 180 days.[24] Second, per Executive Order 13771, federal agencies must identify two existing regulations to be repealed for every new regulation issued during fiscal year 2017, and the order further provides that for each new regulation, the head of the agency is required to identify offsetting regulations and provide the agency's best approximation of the total costs or savings associated with each new regulation or repealed regulation.[25] Despite these challenges, TSA officials stated they plan further actions to update rules related to employee vetting in accordance with this section; however, officials could not provide a timeframe for completing this requirement.

In addition, TSA officials stated they plan no further action with respect to section 3405(b)(1), which requires TSA and the FBI to implement the Rap

[24]In general, agencies promulgating regulations are required to (1) publish a notice of proposed rulemaking (NPRM) in the *Federal Register*, (2) allow interested persons an opportunity to comment on the rulemaking process, (3) issue a final rule accompanied by a statement of its basis and purpose, to include the agency's response to comments received on the NPRM, and (4) publish the final rule at least 30 days before it becomes effective. See generally 5 U.S.C. §§ 551-570a.

[25]See Exec. Order No. 13,771, 82 Fed. Reg. 9339 (Jan. 30, 2017).

Back Service for recurrent vetting of aviation workers.[26] In response to this requirement, TSA coordinated with the FBI to implement the FBI's Rap Back Service, which 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 badge credentials. TSA officials stated the Rap Back program is available to all commercial airport operators; however, for airport operators to participate in the Rap Back program, the airport operator must, among other things, sign a memorandum of understanding with TSA that documents its participation in the program. As of June 2017, TSA had executed over 100 memoranda of understanding with airport operators, including 17 category X airports and plans to enroll additional airports in fiscal year 2017.

Develop and Implement Access Control Metrics (Section 3406)

TSA made progress by taking action on the 6 requirements in Section 3406 of the 2016 ASA. Of the 6 requirements, TSA officials stated they plan no further action to implement the requirements of this section, as shown in appendix I. For example, section 3406 requires TSA to develop and implement performance metrics to measure the effectiveness of security for the SIDAs of airports and, in developing these metrics, TSA may consider 5 factors stated in the Act.[27] In accordance with this requirement, TSA developed and implemented a metric that determines the percentage of TSA SIDA inspections that were found to be in

[26]As part of the requirement to implement the Rap Back service, TSA must ensure that (1) any status notifications the TSA receives through the Rap Back service about criminal offenses be limited to only disqualifying criminal offenses in accordance with the regulations promulgated by the TSA under 49 U.S.C. § 44903, or other federal law; (2) any information received by TSA through the Rap Back service is provided directly and immediately to the relevant airport and aircraft operators. § 3405(b)(2), 130 Stat. at 659-60. Finally, TSA must submit to the appropriate congressional committees a report on such implementation. § 3405(b)(3), 130 Stat. at 660.

[27]In developing the metrics required under this section, TSA may consider: (1) adherence to access point procedures; (2) proper use of credentials; (3) differences in access point requirements between airport workers performing functions in other areas of an airport; (4) difference in access point characteristics and requirements at airports; and (5) any additional factors the Administrator considers necessary to measure performance. § 3406(b), 130 Stat. at 660.

compliance with the airport security program.[28] TSA officials stated they plan to use the metric to inform decision makers on the SIDA compliance for individual airports and nationwide. For example, if TSA determines an individual airport has a low compliance rate, TSA leadership may conduct additional special emphasis inspections to address the issue, according to TSA officials.

Develop a Tool for Unescorted Access Security (Section 3407)

TSA made progress on the 18 requirements in Section 3407 of the 2016 ASA. Of the 18 requirements, TSA plans no further action on 17 requirements, and further action for 1 requirement, as shown in appendix I. For example, section 3407(a) requires TSA to develop a model and best practices for unescorted access security that includes 5 requirements as stated in the Act.[29] In accordance with this requirement, TSA officials stated they utilized a tool for unescorted access security called the Advanced Threat Local Allocation Strategy (ATLAS) tool, which was developed in 2015 and is designed to randomly screen aviation workers who have unescorted access to restricted areas of an airport. The tool incorporates the required elements listed in section 3407(a) such as using intelligence, scientific algorithms and other risk-based factors, according to TSA officials. For example, TSA officials stated the algorithm in the tool provides a scientific way to randomize the locations, times, and types of screening an aviation worker might receive. It allows TSA to limit an individual's ability to circumvent screening by deploying resources in a way that an individual who enters an access point will not know if, or what type of screening will take place, according to officials. While officials stated they plan no further actions to implement the requirements in section 3407(a) to develop a model, officials stated they had conducted pilot assessments of the ATLAS tool in fiscal year 2015 at three airports, at one airport in fiscal year 2016, and plan to pilot the tool in additional

[28]The metric is calculated by the number of TSA inspections that occurred in the SIDA of an airport, or airports, over a set period of time divided by the total number of inspections found to be in compliance during that time period.

[29]Sections 3407(a) requires TSA to develop a model and best practices for unescorted access security that (1) use intelligence, scientific algorithms, and risk-based factors; (2) ensure integrity, accountability, and control; (3) subject airport workers to random physical security inspections conducted by TSA representatives in accordance with this section; (4) appropriately manage the number of the SIDA access points to improve supervision of and reduce unauthorized access to SIDAs and (5) include validation of identification materials, such as with biometrics. § 3407(a)(1)-(5), 130 Stat. at 660-61.

airports before expanding its use in phases to all airports by fiscal year 2018, according to TSA officials.[30]

Increase Covert Testing (Section 3408)

TSA made progress on the 2 requirements in Section 3408 of the 2016 ASA. Of the 2 requirements, TSA plans no further action for 1 requirement, and plans to take further action for 1 requirement, as shown in appendix I. For example, TSA plans further actions to increase the use of covert testing in fiscal year 2017 in accordance with section 3408(a), which requires TSA to increase the use of red-team, covert testing of access controls to any secure areas. Specifically, TSA conducted one access control covert project in fiscal year 2016 and plans to increase the number of projects to three in fiscal year 2017. Additionally, TSA submitted a report on access control covert testing to the appropriate congressional committees as required by section 3408(c)(1) of the 2016 ASA, describing the steps TSA plans to take to expand the use of access control covert testing, and TSA plans no further action to address this reporting requirement.

Review Security Directives (Section 3409)

TSA made progress on the 6 requirements in Section 3409 of the 2016 ASA. Of the 6 requirements, TSA plans no further action on 4 requirements, and plans further action on 2 requirements, as shown in appendix I. Section 3409(a) requires TSA to conduct a comprehensive review of every current security directive addressed to any regulated entity.[31] Section 3409(b) requires TSA to submit notice to the appropriate congressional committees for each new security directive TSA issues.[32] TSA officials stated they have a process in place to review current

[30]In fiscal year 2015, TSA officials stated they conducted pilot assessments at Nashville International Airport, Tennessee; Cincinnati Northern Kentucky Airport, Kentucky; and McCarran International Airport in Nevada. In fiscal year 2016, TSA conducted a pilot assessment at Portland International Airport in Oregon, according to TSA officials.

[31]Specifically, the statute requires TSA to conduct a comprehensive review of every current security directive addressed to any regulated entity to (1) determine whether each such security directive continues to be relevant; (2) determine whether such security directives should be streamlined or consolidated to most efficiently maximize risk reduction; and (3) update, consolidate, or revoke any security directive as necessary. § 3409(a)(1)-(3), 130 Stat. at 662.

[32]See § 3409(b)(1)-(2), 130 Stat. at 662.

security directives. For example, officials stated that they review all current security directives on at least an annual basis, through working groups of TSA and industry association officials. TSA stated these working groups consider, among other things, security directives within airport security programs and the need for revocation or revision of current security directives and TSA plans no further action to address this requirement. With respect to the issuance of new security directives, TSA officials stated they provide briefings for relevant congressional committees as requested regarding the issuance of a new security directive and the rationale for issuing it. According to officials, further action is planned to address these requirements for new security directives.

TSA Identified Two 2016 ASA Requirements that May Specifically Reduce Access Control Vulnerabilities

While TSA officials stated that it is too early to measure the effectiveness of the applicable requirements of the 2016 ASA, they stated that implementing these requirements would broadly have an effect on improving aviation security and identified two requirements that, when implemented, may specifically reduce access control vulnerabilities. First, in accordance with section 3404(a) of the Act, TSA plans to issue a security directive to require airport operators to match the expiration date of an identification badge of an aviation worker that possesses a temporary immigration status with the individual's U.S. work authorization expiration date.[33] TSA officials stated that this measure may help prevent workers who are no longer authorized to work in the United States from inappropriately gaining access to airport SIDAs because an expired identification badge will prevent entry into the SIDA.

Second, in accordance with section 3405(b) of the Act, TSA coordinated with the FBI to implement the Rap Back Service for airport operators to recurrently vet aviation workers in October 2016. The Rap Back service 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 badge credentials. As of June 2017, TSA executed memorandums of understanding with 105 airport operators, including 17 category X airports, and 1 airline, to complete the Rap Back enrollment process. TSA officials stated that implementing the requirement to recurrently vet aviation workers may also reduce vulnerabilities associated with the insider threat. For example, they stated that continuous vetting would increase the potential for TSA and airport operators to be aware of aviation workers who had engaged in potentially disqualifying criminal activity yet continued to hold active identification badges granting access to airport SIDAs.

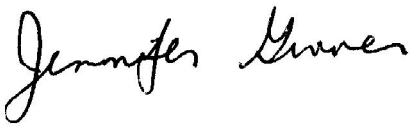
[33] We reviewed a draft of this security directive that aims to address this requirement.

Agency Comments

We provided a draft of this product to the Secretary of Homeland Security for comment. In its formal comments, which are reproduced in full in Appendix II, DHS stated that TSA continues to implement the 2016 ASA requirements. TSA provided technical comments on a draft of this report which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the Secretary of Homeland Security, 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 about this report, please contact Jennifer Grover 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. Key contributors to this report are found in Appendix III.



Jennifer Grover
Director, Homeland Security and Justice

List of Committees

The Honorable John Thune
Chairman
The Honorable Bill Nelson
Ranking Member
Committee on Commerce, Science, and Transportation
United States Senate

The Honorable Ron Johnson
Chairman
The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs
United States Senate

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

Appendix I: TSA's Progress in Implementing the Aviation Security Act of 2016

Subtitle D of the Aviation Security Act of 2016 (ASA),[1] enacted on July 15, 2016, requires the Transportation Security Administration (TSA) to take actions in eight categories that have a total of 69 applicable requirements.[2] The Transportation Security Administration (TSA) has generally made progress addressing the 69 applicable requirements within the 2016 ASA. As of June 2017, TSA officials stated it had implemented 48 of the requirements and plans no further action on these.[3] For 18 requirements, TSA officials took initial actions and plans further action. TSA officials stated they have yet to take action on 2 requirements and plan to address them in the near future. TSA officials took no action on 1 requirement regarding access control rules because it plans to address this through mechanisms other than formal rulemaking, such as drafting a national amendment to airport operator security programs. Because many of TSA's actions taken in response to the 2016 ASA were recently implemented or are still ongoing and not fully implemented, we did not assess the effectiveness of the actions taken by TSA. The tables below present the details of each requirement, the progress made by TSA, and the status of TSA's plans for further action.

Section 3402 of the 2016 ASA requires TSA to, among other things, conduct a threat assessment and submit a report regarding the threat assessment to the appropriate congressional committees. TSA made

[1]Pub. L. No. 114-190, tit. III, subtit. D, 130 Stat. 615, 656-62 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[2]Each category represents a specific section of Subtitle D of the 2016 ASA and each section contains multiple requirements for TSA to implement.

[3]For the status of "no further actions planned", TSA officials believe they fully implemented the requirements as required by the 2016 ASA, or considered the actions identified in the law and determined that no further action was necessary to satisfy the requirement. For the status of "further actions planned", TSA has committed to implementing the requirements through planned actions.

progress in implementing these requirements and has plans for further action, as shown in table 1.

Table 1: Transportation Security Administration's (TSA) Progress Implementing § 3402 of the Aviation Security Act of 2016[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3402(a)(1) Not later than 90 days after the date of the enactment of this Act, the [TSA] Administrator shall conduct or update an assessment to determine the level of risk posed to the domestic air transportation system by individuals with unescorted access to a secure area of an airport [as defined at 49 U.S.C. §44903(j)(2)(H)] in light of recent international terrorist activity.[b]	In October 2016, TSA completed a threat assessment that included an analysis of the threat posed by domestic and international aviation workers who exploit their access privileges to secure areas of an airport to conduct criminal activity.	No Further Action Planned by TSA
§ 3402(a)(2) In conducting or updating the assessment under paragraph (1), the Administrator shall consider—	n/a	n/a
§ 3402(a)(2)(A) domestic intelligence;	TSA's threat assessment included information on incidents occurring at domestic airports, such as specific tactics used.	No Further Action Planned by TSA
§ 3402(a)(2)(B) international intelligence;	TSA's threat assessment included information on incidents overseas such as two attacks that were assessed to have involved the use of insiders.	No Further Action Planned by TSA
§ 3402(a)(2)(C) the vulnerabilities associated with unescorted access authority granted to domestic airport operators and air carriers, and their workers;	TSA's threat assessment included information on joint vulnerability assessments conducted by TSA and the Federal Bureau of Investigation (FBI) at domestic airports.	No Further Action Planned by TSA
§ 3402(a)(2)(D) the vulnerabilities associated with unescorted access authority granted to foreign airport operators and air carriers, and their workers;	TSA's threat assessment included foreign last point of departure data for incoming flights to the United States to determine the likely risk posed by four international regions.	No Further Action Planned by TSA
§ 3402(a)(2)(E) the processes and practices designed to mitigate the vulnerabilities associated with unescorted access privileges granted to airport operators and air carriers, and their workers;	TSA's threat assessment included information on risk mitigation strategies, including how to address potential vulnerabilities.	No Further Action Planned by TSA
§ 3402(a)(2)(F) the recent security breaches at domestic and foreign airports;	TSA's threat assessment included foreign last point of departure data for incoming flights to the United States and recent breaches at domestic airports.	No Further Action Planned by TSA
§ 3402(a)(2)(G) the recent security improvements at domestic airports, including the implementation of recommendations made by relevant advisory committees, including the Aviation Security Advisory Committee (ASAC).	TSA officials stated that they considered but did not include information on recent security improvements and the implementation of ASAC recommendations at domestic airports in its threat assessment because TSA planned to include this information in a separate report required by § 3402(b)(2) of this Act.	No Further Action Planned by TSA
§ 3402(b) The Administrator shall submit to the appropriate congressional committees [c]—	n/a	n/a

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3402(b)(1) a report on the results of the assessment under subsection (a), including any recommendations for improving aviation security;	TSA submitted the report to the appropriate congressional committees in May 2017 with recommendations under consideration for improving aviation security. For example, one recommendation included enhancing relationships with the FBI and U.S. Drug Enforcement Administration, among other law enforcement entities, to ensure TSA is more fully aware of insider threats within the domestic transportation system while another included reviewing and strengthening access control, vetting, and insider threat-related standards.	No Further Action Planned by TSA
§ 3402(b)(2) a report on the implementation status of any recommendations made by the ASAC; and;	TSA officials stated that this report was completed and submitted to the Office of Management and Budget (OMB) for review in December 2016. As of June 2017, TSA officials stated that the report was pending OMB approval and could not provide a date when the report would be submitted to the appropriate congressional committees.	Further Action Planned by TSA
§ 3402(b)(3) regular updates about the insider threat environment as new information becomes available or as needed.	TSA officials stated that they plan to communicate with the appropriate congressional committees to determine how frequently TSA should provide updated insider threat information.	Further Action Planned by TSA

Source: GAO analysis of Transportation Security Administration information | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. § 3402, D, 130 Stat. 615, 656-57 (2016) (enacted on July 15, 2016, as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]49 U.S.C. § 44903(j)(2)(H) provides that "secure area of an airport" means the sterile area and Secure (Security) Identification Display Area of an airport, as those terms are defined at 49 C.F.R. § 1540.5 or any successor regulation.

[c]The Act provides that, "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

Section 3403 of the 2016 ASA required TSA to take actions related to enhancing its oversight activities of aviation workers. TSA made progress in implementing the requirements and has further actions planned, as shown in table 2.

Table 2: Transportation Security Administration's (TSA) Progress Implementing § 3403 of the Aviation Security Act of 2016(2016 ASA)[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3403(a)(1) Subject to public notice and comment, and in consultation with airport operators, the [TSA] Administrator shall update the rules on access controls issued by the Secretary [of Homeland Security] under chapter 449 of title 49, United States Code.	TSA officials stated they took no action to update access control rules. TSA officials stated they took other actions outside of rulemaking, such as drafting a proposed national amendment to airport operator security programs, to address the considerations in this section as noted below.[c]	No Action Planned by TSA
§ 3403(a)(2) As part of the update under paragraph (1), the Administrator shall consider	n/a	n/a
§ 3403(a)(2)(A) increased fines and advanced oversight for airport operators that report missing more than five percent of credentials for unescorted access to any [Security Identification Display Area (SIDA)] of an airport;[b]	TSA officials stated that, prior to the enactment of the 2016 ASA, they could not levy fines on airport operators that reported missing more than five percent of credentials for unescorted access to any SIDA of an airport because TSA did not require airport operators to report this information. TSA officials stated they began to collect this information in October 2016 through inspections of airport operators and have developed a fine structure for airport operators for non-category X airports that have more than five percent of credentials missing for unescorted access to the SIDA of an airport and for category X airports with more than three percent of credentials missing from the SIDA of an airport.[d]	No Further Action Planned by TSA
§ 3403(a)(2)(B) best practices for category X airport operators that report missing more than three percent of credentials for unescorted access to any SIDA of an airport;	In October 2016, TSA developed a list of measures for airport operators to perform and published them on the Department of Homeland Security's Homeland Security Information Network (HSIN) for airport operators to access. TSA is drafting a proposed national amendment to airport operator security programs that will require airport operators to report to TSA when an airport exceeds a specified threshold for unaccounted identification badges.	Further Action Planned by TSA
§ 3403(a)(2)(C) additional audits and status checks for airport operators that report missing more than three percent of credentials for unescorted access to any SIDA of an airport;	TSA is drafting a proposed national amendment to airport operator security programs to report to TSA when an airport exceeds a specified threshold for unaccounted identification badges. Once the amendment is implemented, additional audits of identification badges will be conducted at commercial airports on a yearly basis, according to TSA officials.	Further Action Planned by TSA

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3403(a)(2)(D) review and analysis of the prior five years of audits for airport operators that report missing more than three percent of credentials for unescorted access to any SIDA of an airport;	TSA officials stated that, prior to the enactment of the 2016 ASA, they could not analyze prior year audits of credentials reported missing by airport operators for unescorted access to any SIDA of an airport because TSA did not require airport operators to report this information. TSA officials stated they began collecting this information in October 2016 through inspections of airport operators.	Further Action Planned by TSA
§ 3403(a)(2)(E) increased fines and direct enforcement requirements for both airport workers and their employers that fail to report within 24 hours an employment termination or a missing credential for unescorted access to any SIDA of an airport; and	TSA officials stated they plan to consider proposing increased fines and direct enforcement action requirements for both airport workers and their employers who fail to timely report missing credentials, taking into account the circumstances in accordance with TSA's guidelines for assessing violations, but have yet to do so.	Action Not Yet Taken by TSA
§ 3403(a)(2)(F) a method for termination by the employer of any airport worker who fails to report in a timely manner missing credentials for unescorted access to any SIDA of an airport.	TSA officials stated that they considered a termination method for an aviation worker who failed to report missing credentials but do not plan to take action because TSA does not have authority over employment determinations made by airport operators.[e]	No Further Action Planned by TSA
§ 3403(b) The Administrator may encourage the issuance by airports and aircraft operators of free, one-time, 24-hour temporary credentials for workers who have reported, in a timely manner, their credentials missing, but not permanently lost, stolen, or destroyed, until replacement of credentials under [49 C.F.R. § 1542.211] is necessary.	TSA officials stated that they considered the issuance of temporary credentials for workers who report missing credentials but do not plan to take action because the use of temporary credentials conflicts with an existing federal regulation.[f]	No Further Action Planned by TSA
§ 3403(c) The Administrator shall—	n/a	n/a
§ 3403(c)(1) notify the appropriate congressional committees each time an airport operator reports that more than three percent of credentials for unescorted access to any SIDA at a category X airport are missing, or more than five percent of credentials to access any SIDA at any other airport are missing.[g]	TSA developed a congressional reporting process to notify specific congressional committees on a quarterly basis the number of non-category X airports that have more than five percent of credentials missing for unescorted access to the SIDA of the airport and the number of category X airports with more than three percent of credentials missing from the SIDA of an airport.	No Further Action Planned by TSA
§ 3403(c)(2) submit to the appropriate congressional committees an annual report on the number of violations and fines related to unescorted access to the SIDA of an airport collected in the preceding fiscal year.	TSA submitted a report to the appropriate congressional committees in March 2017 that states that 265 civil violations occurred in cases involving the integrity of the SIDA of an airport. In addition, TSA assessed over $800,000 in civil penalties in these cases. TSA officials said they plan to submit the report on an annual basis.	Further Action Planned by TSA

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, § 3403, 130 Stat. 615, 657-58 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]See 49 C.F.R. § 1540.5 (defining "security identification display area" as "a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.").

[c]As of July 2017, TSA's proposed national amendments cited in this appendix are in draft form. In accordance with 49 C.F.R. § 1542.105, national amendments proposed by TSA require (1) notice to airport operators, in writing, of the proposed amendment while allowing thirty days for the airport operator to provide comment on the amendment; (2) TSA consideration of relevant materials, including comment provided by airport operators and (3) notification by TSA to airport operators of the adoption or rescission of the amendment.

[d]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.

[e]TSA officials stated that while TSA has authority to prohibit the issuance of an identification badge, it does not have authority over airport operators' or other employers' personnel practices.

[f]TSA officials cited 49 C.F.R. § 1542.211 as the regulation that conflicted with this consideration.

[g]The Act provides that, "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

Section 3404 of the 2016 ASA requires TSA to take action on actions related to updating employee credential guidance. TSA made progress in implementing the requirements in this section and plans further actions, as shown in table 3.

Table 3: Transportation Security Administration's (TSA) Progress Implementing § 3404 of the Aviation Security Act of 2016[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3404(a) Not later than 90 days after the date of the enactment of this Act, the [TSA] Administrator shall issue to airport operators guidance regarding placement of an expiration date on each airport credential issued to a non-United States citizen that is not longer than the period of time during which such non-United States citizen is lawfully authorized to work in the United States.	In October 2016, TSA published guidance on the Department of Homeland Security's Homeland Security Information Network (HSIN) for airport operators to match an identification badge's expiration date to an individual's immigration status. TSA plans to further address this requirement with a security directive.[b]	Further Action Planned by TSA
§ 3404(b)(1) Not later than 90 days after the date of the enactment of this Act, the Administrator shall—	n/a	n/a

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3404(b)(1)(A) issue guidance for transportation security inspectors to annually review the procedures of airport operators and air carriers for applicants seeking unescorted access to any [Security Identification Display Area (SIDA)] of an airport;[c] and	TSA officials stated that Transportation Security Inspector guidance is updated yearly to incorporate additional inspection guidelines. According to TSA officials, yearly updates to its Compliance Manual include updated methods for inspections and additional airport access control measures to be tested. TSA officials stated that its Compliance Work Plan, which provides guidance on the number and type of inspections to conduct in the fiscal year, is also updated yearly. According to TSA officials, the plan's fiscal year 2017 update reflects a change in the number of required tests related to insider threats and new inspection techniques related to individuals seeking unescorted access to the SIDA.	No Further Action Planned by TSA
§ 3404(b)(1)(B) make available to airport operators and air carriers information on identifying suspicious or fraudulent identification materials.	TSA developed fraudulent document detection guidance for TSA personnel on (1) types of individuals who seek to use fraudulent documentation and fraudulent documentation creation methods, such as altering a photograph or a document's expiration date; (2) methods for fraudulent documentation detection, such as comparing identification to the person presenting the identification, including facial comparison; and (3) appropriate responses when TSA personnel discover fraudulent documentation. TSA officials stated that this guidance was made available to airport operators to access via the HSIN in fiscal year 2017.	No Further Action Planned by TSA
§ 3404(b)(2) The guidance issued pursuant to paragraph (1) shall require a comprehensive review of background checks and employment authorization documents issued by United States Citizenship and Immigration Services during the course of a review of procedures under such paragraph.	TSA plans to request clarification from the appropriate congressional committees to determine the actions needed to implement this requirement, but have yet to do so.[d]	Action Not Yet Taken by TSA

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, § 3404, 130 Stat. 615, 658 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]As of June 2017, TSA's security directive to address this requirement is in draft form.

[c]See 49 C.F.R. § 1540.5 (defining "security identification display area" as "a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.").

[d]The Act provides that, "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

Section 3405 of the 2016 ASA required TSA to take action on requirements related to vetting aviation workers. TSA made progress in implementing these requirements and plans further action on certain requirements, as shown in table 4.

Table 4: Transportation Security Administration's (TSA) Progress Implementing § 3405 of the Aviation Security Act of 2016[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3405(a)(1) Not later than 180 days after the date of the enactment of this Act, and subject to public notice and comment, the [TSA] Administrator shall revise the regulations issued under [49 U.S.C. § 44936], in accordance with this section and current knowledge of insider threats and intelligence under section 3502 [of this Act], to enhance the eligibility requirements and disqualifying criminal offenses for individuals seeking or having unescorted access to any [Security Identification Display Area (SIDA)] of an airport.[b]	TSA is in the process of revising the regulations. In December 2016, TSA reported that it formed a Rulemaking Integrated Project Team (IPT) to begin the process of modifying the current regulations on disqualifying criminal offenses for individuals seeking or having unescorted access to any SIDA of an airport. The IPT plans to incorporate insider threat information and intelligence in determining TSA's rulemaking decisions and determine which crimes, if any, to propose to add to the current list of disqualifying offenses in the Code of Federal Regulations.	Further Action Planned by TSA
§ 3405(a)(2) In revising the regulations under paragraph (1), the Administrator shall consider adding to the list of disqualifying criminal offenses and criteria the offenses and criteria listed in [19 C.F.R. § 122.183(a)(4) and 49 C.F.R. § 1572.103].[c]	As part of revising the regulations, TSA plans to consider adding to the list of disqualifying criminal offenses by using the criminal offense criteria used for TSA Transportation Worker Identification Credential adjudication and U.S. Customs and Border Protection denial of access determinations.	Further Action Planned by TSA
§ 3405(a)(3) Notwithstanding [49 U.S.C. § 44936(b)], in revising the regulations under paragraph (1) of this subsection, the Administrator shall—	n/a	n/a
§ 3405(a)(3)(A) ensure there exists or is developed a waiver process for approving the issuance of credentials for unescorted access to any SIDA of an airport for an individual found to be otherwise ineligible for such credentials; and	As part of revising the regulations, TSA plans to develop a proposed waiver process for aviation workers that are denied credentials.	Further Action Planned by TSA

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3405(a)(3)(B) consider, as appropriate and practicable— (i) the circumstances of any disqualifying act or offense, restitution made by the individual, Federal and State mitigation remedies, and other factors from which it may be concluded that the individual does not pose a terrorism risk or a risk to aviation security warranting denial of the credential; and (ii) the elements of the appeals and waiver process established under [46 U.S.C. § 70105(c)].	As part of revising the regulations, TSA officials stated they plan to consider the elements of the appeals and waiver process established for adjudicating TSA's Transportation Worker Identification Credential.	Further Action Planned by TSA
§ 3405(a)(4) In revising the regulations under paragraph (1), the Administrator shall propose that an individual be disqualified if the individual was convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense within 15 years before the date of an individual's application, or if the individual was incarcerated for such crime and released from incarceration within five years before the date of the individual's application.	As part of its revising the regulations, TSA plans to propose extending the current 10 year period to 15 years that an individual be disqualified if the individual was convicted, or found not guilty by reason of insanity, of a disqualifying criminal offense before the date of an individual's application.	Further Action Planned by TSA
§ 3405(a)(5) The Administrator shall require an airport or aircraft operator, as applicable, to certify for each individual who receives unescorted access to any SIDA of an airport that— (A) a specific need exists for providing the individual with unescorted access authority; and (B) the individual has certified to the airport or aircraft operator that the individual understands the requirements for possessing a SIDA badge.	TSA plans to draft a national amendment to airport operator security programs to address this requirement.[d]	Further Action Planned by TSA
§ 3405(a)(6) Not later than 90 days after the date of the enactment of this Act, the Administrator shall submit to the appropriate congressional committees a report on the status of the revision to the regulations issued under [49 U.S.C. § 44936], in accordance with this section.[e]	TSA submitted the report, which includes actions TSA has taken to revise the regulations issued under § 44936, to the appropriate congressional committees on December 6, 2016.	No Further Action Planned by TSA
§ 3405(a)(7) Nothing in this subsection may be construed to affect existing aviation worker vetting fees imposed by the TSA.	n/a	n/a

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3405(b)(1) Not later than 90 days after the date of the enactment of this Act, the Administrator and the Director of the Federal Bureau of Investigation (FBI) shall fully implement the Rap Back service for recurrent vetting of eligible TSA-regulated populations of individuals with unescorted access to any SIDA of an airport.	TSA coordinated with the FBI to implement the Rap Back Service for airport operators to recurrently vet aviation workers in October 2016. The Rap Back service 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 badge credentials. For airport operators to participate in the Rap Back program, the airport operator must, among other things, sign a memorandum of understanding with TSA that documents its participation in the program. As of June 2017, TSA executed memorandums of understanding with 105 airport operators, including 17 category X airports, and 1 airline, to complete the Rap Back enrollment process. As of June 2017, airport operators have enrolled over seventy thousand aviation workers.	No Further Action Planned by TSA
§ 3405(b)(2) As part of the requirement in paragraph (1), the Administrator shall ensure that—	n/a	n/a
§ 3405(b)(2)(A) any status notifications the TSA receives through the Rap Back service about criminal offenses be limited to only disqualifying criminal offenses in accordance with the regulations promulgated by the TSA under [49 U.S.C. § 44903], or other Federal law; and	TSA plans to further collaborate with the FBI in order for the FBI to limit the criminal history record information provided to airport operators to only the disqualifying criminal offenses listed under section 44936 of title 49, United States Code.	Further Action Planned by TSA
§ 3405(b)(2)(B) any information received by the Administration through the Rap Back service is provided directly and immediately to the relevant airport and aircraft operators.	The Rap Back service enables TSA and airport operators to receive notification from the FBI's Rap Back Service of criminal offenses for aviation workers on a recurring basis. When the Rap Back service identifies an enrolled individual as having committed a new criminal offense, such as an arrest or conviction, the FBI sends notification of the offense in near real-time to TSA. TSA then processes these results and provides them to the airport operator or airline for adjudication. Adjudication may result in revoking an individual's SIDA badge.	No Further Action Planned by TSA
§ 3405(b)(3) Not later than 30 days after implementation of the Rap Back service described in paragraph (1), the Administrator shall submit to the appropriate congressional committees a report on the such implementation.	TSA submitted the report, which discusses TSA's implementation of the Rap Back service, to the appropriate congressional committees in April 2017.	No Further Action Planned by TSA

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3405(c) Not later than 30 days after the date of the enactment of this Act, the Administrator and the Director of National Intelligence shall coordinate to ensure that the Administrator is authorized to receive automated, real-time access to additional Terrorist Identities Datamart Environment (TIDE) data and any other terrorism-related category codes to improve the effectiveness of the TSA's credential vetting program for individuals who are seeking or have unescorted access to any SIDA of an airport.	TSA coordinated with the National Counterterrorism Center within the Office of the Director of National Intelligence to grant TSA access to additional TIDE data for aviation worker vetting.	No Further Action Planned by TSA
§ 3405(d) Not later than 90 days after the date of the enactment of this Act, the Secretary shall authorize each airport operator to have direct access to the E-Verify program and the Systematic Alien Verification for Entitlements (SAVE) automated system to determine the eligibility of individuals seeking unescorted access to any SIDA of an airport.	Requirement Not Applicable to TSA.	

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, § 3405, 130 Stat. 615, 658-60 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]See 49 C.F.R. § 1540.5 (defining "security identification display area" as "a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.").

[c]See 19 C.F.R. § 122.183(a)(4) (disqualifying criminal offenses for access to a Customs security area) and 49 C.F.R. § 1572.103 (disqualifying criminal offenses for obtaining or renewing a Hazardous Materials Endorsement, or a Transportation Worker Identification Credential).

[d]As of July 2017, TSA's proposed national amendments cited in this appendix are in draft form.

[e]The Act provides that, "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

Section 3406 of the 2016 ASA required TSA to, among other things, develop and implement performance metrics to measure the effectiveness of security for Security Identification Display Areas of airports. TSA made progress in implementing these requirements and plans no further action on all requirements, as shown in table 5.

Table 5: Transportation Security Administration's (TSA) Progress Implementing § 3406 of the Aviation Security Act of 2016[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3406(a) Not later than one year after the date of the enactment of this Act, the [TSA] Administrator shall develop and implement performance metrics to measure the effectiveness of security for the [Security Identification Display Areas (SIDA)] of airports.[b]	TSA developed and implemented a metric that determines the percentage of TSA inspections of a SIDA that were found to be in compliance with airport security programs.[c]	No Further Action Planned by TSA
§ 3406(b) In developing the performance metrics under subsection (a), the Administrator may consider—	n/a	n/a
§ 3406(b)(1) adherence to access point procedures;	TSA incorporated the adherence to access point procedures into the metric.	No Further Action Planned by TSA
§ 3406(b)(2) proper use of credentials;	TSA incorporated the proper use of credentials into the metric.	No Further Action Planned by TSA
§ 3406(b)(3) differences in access point requirements between airport workers performing functions on the airside of an airport and airport workers performing functions in other areas of an airport;	TSA officials stated they considered the differences in access point requirements between airport workers performing functions in different parts of an airport but chose not to incorporate this information into the metric because incorporating this information would not be consistent with how TSA plans to use the metric for decision making.	No Further Action Planned by TSA
§ 3406(b)(4) differences in access point characteristics and requirements at airports; and	TSA officials stated they considered the differences in access point characteristics and requirements at airports but chose not to incorporate this information into the metric because incorporating this information would not be consistent with how TSA plans to use the metric for decision-making.	No Further Action Planned by TSA
§ 3406(b)(5) any additional factors the Administrator considers necessary to measure performance.	TSA officials stated they did not consider it necessary to include additional factors into the metric.	No Further Action Planned by TSA

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, § 3406, 130 Stat. 615, 660 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]See 49 C.F.R. § 1540.5 (defining "security identification display area" as "a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.").

[c]The metric is calculated by the number of TSA inspections that occurred in the SIDA of an airport, or airports, over a set period time divided by the total number of inspections found to be in compliance during that time period.

Section 3407 of the 2016 ASA requires TSA to, among other things, develop a model and best practices for unescorted access security. TSA made progress in implementing these requirements and plans further action on certain requirements, as shown in table 6.

Table 6: Transportation Security Administration's (TSA) Progress Implementing § 3407 of the Aviation Security Act of 2016(2016 ASA)[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3407(a) Not later than 180 days after the date of the enactment of this Act, the [TSA] Administrator, in consultation with the [Aviation Security Advisory Committee (ASAC)] shall develop a tool and best practices for unescorted access security that -	TSA developed the Advanced Threat Local Allocation Strategy (ATLAS) tool that uses an algorithm to randomize the location, time, and type of screening aviation workers who have access to the secure areas of an airport receive. TSA piloted the tool in fiscal year 2015 at Nashville International Airport, Tennessee; Cincinnati Northern Kentucky International Airport, Kentucky; and McCarran International Airport in Nevada. In fiscal year 2016, TSA conducted a pilot assessment at Portland International Airport, Oregon.	No Further Action Planned by TSA
§ 3407(a)(1) use intelligence, scientific algorithms, and risk-based factors;	The ATLAS tool, developed by TSA, uses intelligence, an algorithm, and other risk-based factors; such as randomizing the location, time, and type of screening when screening aviation workers. TSA officials stated the algorithm applies weighted randomization of location, time and type of screening. The tool is designed to ensure that aviation workers with unescorted access are randomly screened for prohibited items, such as firearms and explosives, and to check for proper identification, according to TSA officials.	No Further Action Planned by TSA
§ 3407(a)(2) ensure integrity, accountability, and control;	TSA officials stated that the ATLAS tool can be customized by TSA officials at each individual airport to ensure proper control and integrity of randomized inspections.	No Further Action Planned by TSA
§ 3407(a)(3) subject airport workers to random physical security inspections conducted by TSA representatives in accordance with this section;	TSA officials stated the ATLAS tool randomizes the location, time and type of screening, and will subject airport workers to random physical security inspections.	No Further Action Planned by TSA
§ 3407(a)(4) appropriately manage the number of the [Security Identification Display Areas (SIDA)] access points to improve supervision of and reduce unauthorized access to SIDAs;[b] and	TSA officials stated the one of the objectives of the ATLAS tool is to reduce unauthorized access to the SIDA of an airport by inspecting these access points randomly.	No Further Action Planned by TSA
§ 3407(a)(5) include validation of identification materials, such as with biometrics.	TSA officials stated that when aviation workers are screened randomly, they will be required to present valid identification materials.	No Further Action Planned by TSA

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3407(b) Consistent with a risk-based security approach, the Administrator shall expand the use of transportation security officers and inspectors to conduct enhanced, random and unpredictable, data-driven, and operationally dynamic physical inspections of airport workers in each SIDA of an airport and at each SIDA access point to—	Prior to the 2016 ASA, TSA increased the frequency of physical inspections for aviation workers. In addition, TSA plans to incorporate ATLAS into airports nationwide. TSA officials stated the ATLAS tool uses an algorithm to randomize the location, time, and type of screening type aviation workers receive. The type of screening is designed to be unpredictable and to be used at all SIDAs of airports.	Further Action Planned by TSA
§ 3407(b)(1) verify the credentials of such airport workers;	TSA officials stated transportation security officers currently conduct random screening activities and ID challenges to ensure individuals are authorized to be in secure areas of an airport.	No Further Action Planned by TSA
§ 3407(b)(2) determine whether such airport workers possess prohibited items, except for those items that may be necessary for the performance of such airport workers' duties, as appropriate, in any SIDA of an airport; and	TSA officials stated insider threat teams currently conduct screening to potentially discover prohibited items.	No Further Action Planned by TSA
§ 3407(b)(3) verify whether such airport workers are following appropriate procedures to access any SIDA of an airport.	TSA officials stated insider threat teams conduct screening by conducting ID media verification checks after an individual submits him or herself for security screening at direct access points	No Further Action Planned by TSA
§ 3407(c)(1) The Administrator shall conduct a review of airports that have implemented additional airport worker screening or perimeter security to improve airport security, including—	TSA stated that they reviewed the local procedures and costs for three airports—Atlanta Hartsfield, Miami International, and Orlando International airports—that have implemented additional airport worker screening.	No Further Action Planned by TSA
§ 3407(c)(1)(A) comprehensive airport worker screening at access points to secure areas;[c]	TSA stated that they reviewed local procedures and costs associated with screening virtually 100 percent of aviation workers at Atlanta Hartsfield, Miami International, and Orlando International airports.	No Further Action Planned by TSA
§ 3407(c)(1)(B) comprehensive perimeter screening, including vehicles;	TSA officials stated TSA annually conducts a comprehensive inspection of each TSA-regulated airport's security program, which includes perimeter and vehicle screening. In an information circular dated March 2017, TSA encouraged all airports to perform comprehensive vulnerability assessments of their perimeter security and vehicles, among other items.	No Further Action Planned by TSA

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3407(c)(1)(C) enhanced fencing or perimeter sensors; and	TSA officials stated TSA annually conducts a comprehensive inspection of each TSA-regulated airport's security program, which includes perimeter and vehicle screening. In an information circular dated March 2017, TSA encouraged all airports to perform comprehensive vulnerability assessments of their perimeter security and vehicles, among other items.	No Further Action Planned by TSA
§ 3407(c)(1)(D) any additional airport worker screening or perimeter security measures the Administrator identifies.	TSA officials stated that TSA solicits industry feedback through several venues, such as its Quarterly Airport Security Reviews that identifies best practices in airport security, including employee screening and perimeter security.[d]	No Further Action Planned by TSA
§ 3407(c)(2) After completing the review under paragraph (1), the Administrator shall—	n/a	n/a
§ 3407(c)(2)(A) identify best practices for additional access control and airport worker security at airports; and	In October 2016, TSA developed a list of measures, such as additional access controls, for airport operators to perform and published them on the Department of Homeland Security's Homeland Security Information Network (HSIN) for airport operators to access. In addition, TSA officials stated they spoke with airport operators on a national call in May 2017 to discuss and identify best practices for access control and airport worker security.	No Further Action Planned by TSA
§ 3407(c)(2)(B) Disseminate to airport operators the best practices identified under subparagraph (A).	In October 2016, TSA published a list of measures, such as additional access controls for airport operators to perform, and published them on the HSIN for airport operators to access.	No Further Action Planned by TSA
§ 3407(c)(3) The Administrator may conduct a pilot program at one or more airports to test and validate best practices for comprehensive airport worker screening or perimeter security under paragraph (2).	TSA officials stated that several assessments, including by the Aviation Security Advisory Committee in 2015, found that 100% physical screening of aviation workers is cost prohibitive and does not significantly increase protection or lower risk. As a result, TSA officials stated they plan no action to conduct additional pilot programs using 100% aviation worker screening.	No Further Action Planned by TSA

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, 130 Stat. § 3407, 615, 660-61 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]See 49 C.F.R. § 1540.5 (defining "security identification display area" as "a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.").

[c]49 U.S.C. § 44903(j)(2)(H) provides that "secure area of an airport" means the sterile area and Secure (Security) Identification Display Area of an airport, as those terms are defined at 49 C.F.R. § 1540.5 or any successor regulation.

[d]TSA officials stated that TSA and industry associations formed a working group—the Quarterly Airport Security Review—to review all active security directives which include, among other topics, airport worker screening and perimeter security.

Section 3408 of the 2016 ASA requires TSA to, among other things, increase the use of red-team covert testing of access controls to any secure areas of an airport. TSA made progress in implementing these requirements and plans further action on certain requirements, as shown in table 7.

Table 7: Transportation Security Administration's (TSA) Progress Implementing § 3408 of the Aviation Security Act of 2016[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3408(a) The Administrator shall increase the use of red-team, covert testing of access controls to any secure areas of an airport.[b]	From fiscal year 2016 to fiscal year 2017, TSA plans to increase the use of access control covert testing projects for secure areas of an airport.	Further Action Planned by TSA
§ 3408(b) Additional Covert Testing—The Inspector General of the Department of Homeland Security shall conduct red-team, covert testing of airport access controls to the [Security Identification Display Areas (SIDA)] of airports.[c]	Requirement not applicable to TSA.	n/a
§ 3408(c)(1) Not later than 90 days after the date of the enactment of this Act, the Administrator shall submit to the appropriate congressional committees a report on the progress to expand the use of inspections and of red-team, covert testing under subsection (a).[d]	In December 2016, TSA submitted the report to the appropriate congressional committees, which includes steps TSA plans to take to expand the use of red team, covert testing.	No Further Action Planned by TSA
§ 3408(c)(2) Inspector general report—Not later than 180 days after the date of the enactment of this Act, the Inspector General of the Department of Homeland Security shall submit to the appropriate congressional committees a report on the effectiveness of airport access controls to the SIDAs of airports based on red-team, covert testing under subsection (b).	Requirement not applicable to TSA.	n/a

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, § 3408, 130 Stat. 615, 661-62 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]49 U.S.C. § 44903(j)(2)(H) provides that "secure area of an airport" means the sterile area and Secure (Security) Identification Display Area of an airport, as those terms are defined at 49 C.F.R. § 1540.5 or any successor regulation.

[c]See 49 C.F.R. § 1540.5 (defining "security identification display area" as "a portion of an airport specified in the airport security program, in which security measures specified in this part are carried out. This area includes the secured area and may include other areas of the airport.").

[d]The Act provides that, "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

Section 3409 of the 2016 ASA requires TSA to, among other things, review all security directives to determine if they remain relevant, and report to Congress on security directives. TSA made progress in implementing these requirements and plans further action on certain requirements, as shown in table 8.

Table 8: Transportation Security Administration's (TSA) Progress Implementing § 3409 of the Aviation Security Act of 2016[a]

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3409(a) Not later than 180 days after the date of the enactment of this Act and annually thereafter, the [TSA] Administrator, in consultation with the appropriate regulated entities, shall conduct a comprehensive review of every current security directive addressed to any regulated entity to[b]—	TSA officials stated that they currently review all security directives on at least an annual basis, through working groups of TSA and industry association officials. TSA officials stated that among other things, these working groups consider the placement of security directives within airport security programs and the need for deletion or revision of current security directives.	No Further Action Planned by TSA
§ 3409(a)(1) determine whether each such security directive continues to be relevant;	TSA officials stated they continue to review the security directives to determine if they remain relevant.	No Further Action Planned by TSA
§ 3409(a)(2) determine whether such security directives should be streamlined or consolidated to most efficiently maximize risk reduction; and	TSA officials stated they continue to review each security directive to determine whether the security directive reduces risks to aviation security.	No Further Action Planned by TSA
§ 3409(a)(3) update, consolidate, or revoke any security directive as necessary.	TSA officials stated they continue to update, consolidate, or revoke security directives that are deemed no longer necessary to aviation security.	No Further Action Planned by TSA
§ 3409(b) For each security directive that the Administrator issues, the Administrator shall submit to the appropriate congressional committees notice of—[c]	n/a	n/a
§ 3409 (b)(1) the extent to which each such security directive responds to a specific threat, security threat assessment, or emergency situation against civil aviation; and	TSA officials stated they plan to provide notice to the appropriate congressional committees when TSA issues a security directive. As part of the notice, TSA plans to provide the rationale for issuing the security directive as well as the security directive's expiration date.	Further Action Planned by TSA

Statute	TSA's Progress Implementing the Aviation Security Act of 2016	Status
§ 3409 (b)(2) when it is anticipated that each such security directive will expire.	TSA officials stated they plan to provide notice to the appropriate congressional committees when TSA issues a security directive. As part of the notice, TSA plans to provide the rationale for issuing the security directive as well as the security directive's expiration date.	Further Action Planned by TSA

Source: GAO analysis of Transportation Security Administration information. | GAO 17-662

[a]Pub. L. No. 114-190, tit. III, subtit. D, § 3409, 130 Stat. 615, 662 (2016) (enacted on July 15, 2016 as part of Title III of the FAA Extension, Safety, and Security Act of 2016).

[b]TSA may 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).

[c]The Act provides that, "appropriate congressional committees" means the Committee on Homeland Security of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, and the Committee on Commerce, Science, and Transportation of the Senate. § 3401(1), 130 Stat. at 656.

Appendix II: Comments from the Department of Homeland Security

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

Homeland Security

August 18, 2017

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

Re: Management's Response to Draft Report GAO-17-662, "AVIATION SECURITY: TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016"

Dear Ms. Grover:

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

The Department is pleased to note GAO's positive recognition of the Transportation Security Administration's (TSA) diligent efforts to comply with the requirements of the Aviation Security Act of 2016. As the report highlights, TSA has made significant progress in thwarting the insider threat from aviation workers who may "exploit their access privileges to secure areas of an airport for personal gain or to inflict damage." TSA remains committed to staying ahead of evolving threats and raising the baseline for aviation security to ensure the security of airline passengers, the public, and the nation's airports.

Working in partnership with the Aviation Security Advisory Council and other stakeholders, TSA has implemented 48 of the 69 requirements of the Act. TSA has developed policy documents, guidelines, metrics, and assessment tools to support increased access control measures in response to insider threat concerns. TSA is placing a high priority on actions underway or planned to implement the remaining requirements. DHS values GAO's recognition of the progress TSA has made to address key provisions of the Act. We also noted that the report did not include any recommendations.

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
Director
Departmental GAO-OIG Liaison Office

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

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

Acknowledgments

In addition to the contact named above, Kevin Heinz (Assistant Director), Brandon Jones (Analyst-in-Charge), Michele Fejfar, Tyler Kent, Thomas Lombardi, Heidi Nielson, and Claire Peachey made significant contributions to the report.

Appendix IV: Accessible Data

Agency Comment Letter

Accessible Text for Appendix II: Comments from the Department of Homeland Security

August 18, 2017

Ms. Jennifer Grover

Director, Homeland Security and Justice Issues

U.S. Government Accountability Office

441 G Street, NW

Washington, DC 20548

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

Homeland Security

Re: Management's Response to Draft Report GAO-17-662, "AVIATION SECURITY: TSA Has Made Progress Implementing Requirements in the Aviation Security Act of 2016"

Dear Ms. Grover:

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

The Department is pleased to note GAO's positive recognition of the Transportation Security Administration's (TSA) diligent efforts to comply with the requirements of the Aviation Security Act of 2016. As the report highlights, TSA has made significant progress in thwarting the insider threat from aviation workers who may "exploit their access privileges to secure areas of an airport for personal gain or to inflict damage." TSA

remains committed to staying ahead of evolving threats and raising the baseline for aviation security to ensure the security of airline passengers, the public, and the nation's airports.

Working in partnership with the Aviation Security Advisory Council and other stakeholders, TSA has implemented 48 of the 69 requirements of the Act. TSA has developed policy documents, guidelines, metrics, and assessment tools to support increased access control measures in response to insider threat concerns. TSA is placing a high priority on actions underway or planned to implement the remaining requirements. DHS values GAO's recognition of the progress TSA has made to address key provisions of the Act. We also noted that the report did not include any recommendations.

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

Director

Departmental GAO-OIG Liaison Office

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, LinkedIn, Twitter, and YouTube. Subscribe to our RSS Feeds or E-mail Updates. Listen to our Podcasts. Visit GAO on the web at www.gao.gov and read The Watchblog.

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

Strategic Planning and External Liaison

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