



Testimony
Before the Subcommittee on
Transportation Security, Committee on
Homeland Security, House of
Representatives

For Release on Delivery
Expected at 10:00 a.m. ET
Tuesday, June 16, 2015

AVIATION SECURITY

TSA Has Taken Steps to Improve Vetting of Airport Workers

Statement of Jennifer Grover, Director, Homeland
Security and Justice

Accessible Version

GAO Highlights

Highlights of [GAO-15-704T](#), a testimony before the Subcommittee on Transportation Security, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Since the attacks of September 11, 2001, exposed vulnerabilities in the nation's aviation system, DHS has taken steps to vet airport workers to reduce the security risks they may pose at the approximately 450 commercial airports in the United States. According to TSA, the threat to civil aviation has not diminished—underscoring the need for effective airport worker screening programs. GAO previously reported on TSA's implementation of its Aviation Workers Program in which TSA and airports, in collaboration with the FBI, vet applicants against the FBI's criminal history records, terrorist watchlists and other databases, and issue credentials to qualifying airport workers.

This testimony describes the role of TSA and airports in assessing airport workers for potential security threats, as well as challenges and recent improvements in vetting airport workers. This statement is based on a report and testimonies issued from December 2011 through June 2015, and selected updates in June 2015. For prior work, GAO analyzed TSA documents and interviewed TSA officials. For DHS's recent efforts to vet airport workers, we reviewed applicable policies and an April 2015 report on improving airport employee access control.

What GAO Recommends

GAO previously made recommendations to DHS to strengthen TSA's implementation of its Aviation Workers Program. DHS agreed and took actions to address them. GAO is not making any new recommendations in this testimony.

View [GAO-15-704T](#). For more information, contact Jennifer Grover at (202) 512-7141 or groverj@gao.gov.

June 16, 2015

AVIATION SECURITY

TSA Has Taken Steps to Improve Vetting of Airport Workers

What GAO Found

The Transportation Security Administration (TSA), within the Department of Homeland Security (DHS), requires that before airport operators issue credentials to applicants seeking unescorted access to secure areas of an airport, the applicant must be vetted in accordance with TSA requirements, which generally includes a Security Threat Assessment. GAO reported in December 2011 that this assessment includes checks of criminal history records and immigration status, as well as a check against terrorist databases. To initiate the Security Threat Assessment, airport operators collect applicant information and transmit the results to TSA. TSA adjudicates the immigration and terrorism checks, initiates an automated check of Federal Bureau of Investigation (FBI) criminal history records, and transmits the results of the criminal history record checks to the airport operators. The airport operators are responsible for adjudicating the criminal history to identify potentially disqualifying criminal offenses specified under TSA regulations, and making a final determination of eligibility for a credential.

TSA has taken steps to ensure that airport workers who require unescorted access to secure areas of commercial (i.e., TSA-regulated) airports are properly vetted to ensure they do not pose a security threat. However, GAO previously found that TSA faced challenges in ensuring it had the necessary criminal information to effectively conduct Security Threat Assessments for aviation workers. In December 2011, GAO found that limitations in TSA's criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Security Threat Assessments for airport workers. TSA reported that its ability to review applicant criminal history records was often incomplete due to its status as a noncriminal justice agency. GAO found that TSA and FBI had not assessed whether a potential security risk in TSA's Security Threat Assessment process could exist as a result. As a result, GAO recommended that the TSA and the FBI jointly assess the extent to which this limitation may pose a security risk, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative. TSA and the FBI have since taken steps to address this recommendation. As of September 2014, TSA officials reported that the FBI has taken steps to expand the criminal history record information available to TSA when conducting its Security Threat Assessments for airport workers and others. In April 2015, the Secretary of DHS stated that until TSA establishes a system for "real-time recurrent" criminal history records checks for all airport workers beyond their time of initial employment, the agency shall require fingerprint-based criminal history records checks every two years for such workers with unescorted access to secure areas of the airport. TSA subsequently updated existing requirements to implement procedures consistent with the Secretary's statement.

Chairman Katko, Ranking Member Rice, and Members of the Subcommittee:

I am pleased to be here today to discuss our past work examining the Transportation Security Administration's (TSA) Aviation Workers Program. It has been nearly 14 years since the attacks of September 11, 2001, exposed vulnerabilities in the nation's civil aviation system. Since then, TSA, within the Department of Homeland Security (DHS), has taken steps to ensure that airport workers who require unescorted access to secure areas of commercial (i.e., TSA-regulated) airports are properly vetted to identify those who may pose a security threat. These efforts are intended to reduce the probability of a successful terrorist or other criminal attack at the nation's approximately 450 commercial airports. However, TSA has faced challenges in obtaining the necessary information to accurately assess aviation workers. According to TSA, the threat to civil aviation has not diminished—underscoring the need for effective airport worker screening programs.

As requested, my testimony today describes the role of TSA and airport operators in assessing aviation workers for potential security threats, as well as challenges and recent improvements. In carrying out this process, TSA and airports work in collaboration with the Federal Bureau of Investigation (FBI) to vet applicants against the FBI's criminal history records, terrorist watch lists and other databases, and issue credentials to qualifying airport facility workers, retail employees, and airline employees, among others. This statement is based on our report and testimonies issued from December 2011 through June 2015 related to TSA's efforts to vet aviation workers.¹ For our past work, we reviewed applicable laws, regulations, and policies as well as TSA program documents, decision memorandums, and other documents. We interviewed DHS, TSA, and FBI officials. We also conducted selected updates in June 2015 on recent DHS and TSA efforts to vet aviation workers. For these recent DHS and TSA efforts, we reviewed applicable policies and the Aviation Security Advisory Committee's (ASAC) April 2015 report on improving airport

¹See GAO, *Transportation Security: Actions Needed to Address Limitations in TSA's Transportation Worker Security Threat Assessments and Growing Workload*, [GAO-12-60](#) (Washington, D.C.: Dec. 8, 2011); *Aviation Security: TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed*, [GAO-15-559T](#) (Washington, D.C.: May 13, 2015); and *Aviation Security: TSA Has Taken Steps to Improve Oversight of Key Programs, but Additional Actions Are Needed*, [GAO-15-678T](#) (Washington, D.C.: June 9, 2015).

employee access control.² We reviewed the report's methodology and determined that the findings were reasonable for use in our report. Further details on the scope and methodology for the previously issued report and testimonies are available within each of the published products. We conducted the work on which this statement is based in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

In accordance with the Aviation and Transportation Security Act (ATSA), enacted following the September 11, 2001, terrorist attacks, TSA requires that airport operators (e.g., an airport authority) undertake specific actions before issuing credentials to airport workers seeking unescorted access to secure areas of an airport to reduce potential security risks posed by these workers.³ For example, a worker seeking unescorted access to a Security Identification Display Area (SIDA) must first undergo a fingerprint-based criminal history record check.⁴ TSA oversees implementation of these requirements through its Aviation Workers Program, which focuses on identifying security threats posed by those individuals seeking to obtain a credential for unescorted access to secure or restricted areas of airports. Specifically, TSA, in collaboration with airport operators and the FBI, completes applicant background checks, including Security Threat Assessments, for airport facility workers, retail employees, airline employees, and any other workers who apply for or

²See ASAC, *Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control* (Arlington, VA: April 8, 2015).

³See generally 49 C.F.R. pt. 1542, subpt. C. In general, secure areas of the airport include areas specified in an airport's security program (1) where air carriers enplane and deplane passengers, sort and load baggage, and any adjacent areas (secured areas), (2) in which appropriate identification must be worn (SIDAs), (3) that provide passengers access to boarding aircraft and to which access is general controlled through the screening of persons and property (sterile areas), and (4) that include aircraft movement areas, aircraft parking areas, loading ramps, and safety areas that are not separated by adequate security systems, measures, or procedures (air operations areas). See 49 C.F.R. § 1540.5.

⁴See 49 C.F.R. § 1542.205.

are issued a credential for unescorted access to secure areas in U.S. airports. In general, Security Threat Assessments include checks for criminal history records and immigration status, checks against terrorism databases and watch lists, and checks for records indicating an adjudication of lack of mental capacity, among other things.

TSA and Airport Operators Share Responsibilities for Aviation Worker Vetting

TSA and airport operators each have certain responsibilities within the credentialing process. For example, we reported in December 2011 that airport operators are responsible for ensuring the collection of application information, transmitting the results to TSA for the Security Threat Assessment, enrolling approved applicants, and issuing credentials.⁵ TSA's roles include adjudicating the immigration and terrorism checks, running automated FBI criminal history records, and transmitting the results of the criminal history record checks to the airport operators. The FBI's criminal history records contain information from a national fingerprint and criminal history system.⁶ If an individual has a criminal record in the database, the FBI provides the criminal history record check results to TSA. TSA, in turn transmits the results to the airport operator. The airport operators are responsible under TSA regulations for adjudicating the criminal history to identify potentially disqualifying criminal offenses specified under TSA regulations, and making a final determination of eligibility for a credential.⁷ In doing so, airport operators may follow up with an applicant if the FBI Record of Arrests and Prosecutions (RAP) sheet TSA provided lacks a disposition of a criminal offense—which is necessary for the airport operators to determine if the applicant has potentially disqualifying criminal offenses.⁸ Furthermore,

⁵[GAO-12-60](#).

⁶The system provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses. A segment of this system is the FBI-maintained criminal history record repository, known as the Interstate Identification Index (III, or Triple I) system that contains records from all states and territories, as well as from federal and international criminal justice agencies. The state records in the III are submitted to the FBI by central criminal record repositories that aggregate criminal records submitted by most or all of the local criminal justice agencies in their jurisdictions. The FBI's criminal history records check is a negative identification check, whereby the fingerprints are used to confirm that the associated individual is not identified as having a criminal record in the database.

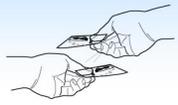
⁷See, e.g., 49 C.F.R. § 1542.209.

⁸See appendix I for a list of TSA Aviation Worker disqualifying criminal offenses.

airport operators, and not TSA, are the entities responsible for revoking the issued credentials.⁹ For example, airport operators are to revoke a worker's credentials if TSA determines the worker poses a threat or violates airport security policy. Figure 1 summarizes the credentialing processes and respective responsibilities of TSA and airport operators under TSA's Aviation Workers Program.

⁹If TSA determines that an individual poses a threat based on checks of information in the Terrorist Screening Database or immigration checks, TSA will notify the airport operator to revoke the credential.

Figure 1: Summary of Credentialing Processes and Responsibilities for TSA and Airport Operators under TSA's Aviation Workers Program

Transportation Security Administration (TSA) and airport operator credentialing responsibilities under TSA Aviation Worker Program		
TSA		Airport operator
Enrollment		
		Applicant provides biographic and biometric information to airport operator. Airport operator submits information to TSA.
Background check		
	TSA vets and adjudicates terrorist and immigration information, and provides results of criminal history checks to airport operator.	Airport operator adjudicates criminal history and makes determination of eligibility.
Issuance		
		Airport operator issues access badge to employee.
Verification		
		Airport operators responsible for implementing access control system as part of TSA-approved security plan.
Renewal		
	In April 2015, TSA modified existing requirements to address the need for recurrent criminal history checks.	As part of the renewal process, the expiring badge must be retrieved by the airport operator.
Revocation		
		Airport operators can revoke a badge if an individual is no longer employed by airport employer, or if an airport is informed by TSA of derogatory information related to immigration status or during recurring criminal history records or recurring terrorist screening checks.

Source: GAO analysis of Department of Homeland Security information; Art Explosion (clip art). | GAO-15-704T

TSA Has Taken Actions to Address Limitations in Aviation Worker Vetting

Criminal history record checks are a key element of the Security Threat Assessment process for TSA's Aviation Worker Program, helping to ensure that the agency and airport operators detect those applicants with potentially disqualifying criminal offenses. However, TSA has faced challenges in ensuring it has the necessary criminal information to effectively conduct Security Threat Assessments for applicants to its Aviation Workers Program. In December 2011, we found that, according to TSA, limitations in its criminal history checks increased the risk that the agency was not detecting potentially disqualifying criminal offenses as part of its Security Threat Assessments for airport workers.¹⁰ Specifically, we found that TSA's level of access to criminal history record information in the FBI's Interstate Identification Index excluded access to many state records such as information regarding sentencing, release dates, and probation or parole violations, among others. For the purposes of accessing criminal history records, FBI provided TSA the level of a noncriminal justice requestor (e.g., equal to that of a private company conducting an employment check on a new applicant, according to TSA). As a result, TSA reported that its access to and airports' ability to review applicant criminal history records was often incomplete. We found that TSA and the FBI had not assessed whether a potential security risk in TSA's Security Threat Assessment process existed with the level of access to FBI criminal records that TSA had at the time.

We recommended that the TSA and the FBI jointly assess the extent to which this limitation may pose a security risk, identify alternatives to address any risks, and assess the costs and benefits of pursuing each alternative. In May 2015 and June 2015, we reported that TSA and the FBI have since taken steps to address this recommendation. For example, in 2014, the agencies concluded that the risk of incomplete information did exist and could be mitigated through expanded access to state-supplied records.¹¹ TSA officials reported that the FBI has since taken steps to expand the criminal history record information available to TSA when conducting its Security Threat Assessments for airport workers and others. For example, TSA reported that the study between the FBI and TSA culminated in the FBI implementing system changes to provide the TSA with access to expanded criminal history record information. According to TSA officials, the FBI's release of its Next Generation

¹⁰GAO-12-60.

¹¹GAO-15-559T and GAO-15-678T.

Identification System—which the FBI reported achieving full operational capability in September 2014—has been enhanced to expand the state-provided criminal history records that are now incorporated into all FBI criminal history record information for TSA’s Security Threat Assessments for aviation workers.¹² We have not evaluated TSA’s use of the new system.

Further, in April 2015, TSA updated existing requirements to address the need for recurrent criminal history records checks for credentialed airport workers with unescorted access to secure airport areas at periodic intervals. Until recently, TSA did not require periodic criminal history checks of workers with unescorted access authority as long as workers maintain continuous employment with the same issuing authority. TSA updated its requirements in response to the ASAC’s recommendation and the Secretary of DHS’s statement regarding airport security enhancements.¹³ ASAC recommended that TSA should incorporate real-time criminal activity monitoring into the aviation worker vetting process in its final report on improving airport employee access control. ASAC found that TSA’s practice of reviewing criminal history records once—at the time of vetting for initial employment—created the potential for TSA and airport operators to be unaware of aviation workers who had subsequently engaged in potentially disqualifying criminal activity yet continued to hold active credentials. ASAC reported that real-time criminal activity monitoring should be a part of the vetting process, similar to the perpetual vetting of aviation workers conducted by TSA against terrorist watch lists. Specifically, ASAC recommended that TSA accelerate implementation of a pilot of criminal activity monitoring using FBI’s Rap Back Service, with a

¹²According to the FBI, the Next Generation Identification System is an incremental replacement of a previous fingerprint identification system that provides new functionality and improves existing capabilities. The technological upgrade accommodates increased information processing and sharing demands from local, state, tribal, federal, and international agencies.

¹³ASAC, at the request of TSA in January 2015, created a working group comprised of representatives from the aviation industry tasked with analyzing the adequacy of existing security measures and recommending any additional measures needed to improve employee access controls. See 49 U.S.C. § 44946 (requiring establishment of an ASAC within TSA to provide advice and recommendations on aviation security matters, including the development, refinement, and implementation of policies, programs, rulemaking, and security directives pertaining to aviation security, while adhering to sensitive security guidelines).

goal of full implementation of the service by the end of 2015.¹⁴ The Secretary of DHS stated that until TSA establishes a system for real-time recurrent criminal history records checks for all aviation workers, TSA should require fingerprint-based criminal history records checks periodically for all airport employee SIDA badge-holders.

Chairman Katko, Ranking Member Rice, and members of the subcommittee, this completes my prepared statement. I would be pleased to respond to any questions that you may have at this time.

For questions about this statement, 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 statement. Individuals making key contributions to this statement include Chris Ferencik (Assistant Director), Elizabeth Luke, Jason Berman, Tom Lombardi, and Michele Fejfar. Key contributors for the previous work that this testimony is based on are listed in each product.

¹⁴FBI introduced its Rap Back Service in September 2014 as part of its Next Generation Identification System. According to the FBI, the Rap Back Service provides users, such as airport authorities, the capability to receive immediate notification of criminal and, in limited cases, civil activity of enrolled individuals that occur after the initial processing and retention of criminal or civil fingerprint transactions, such as the fingerprint-based criminal history records checks currently conducted by TSA and airport operators.

Appendix I: Criminal Offenses That Disqualify Applicants under the Aviation Workers Program from Acquiring an Airport-Issued Badge

In accordance with 49 C.F.R. §§ 1542.209, 1544.229, and 1544.230, an individual has a disqualifying criminal offense if the individual has been convicted, or found not guilty of by reason of insanity, of any of the crimes listed below in any jurisdiction during the 10 years before the date of the individual's application for unescorted access authority, or while the individual has unescorted access authority.

Disqualifying criminal offenses.

1. Forgery of certificates, false marking of aircraft, and other aircraft registration violation; 49 U.S.C. § 46306.
2. Interference with air navigation; 49 U.S.C. § 46308.
3. Improper transportation of a hazardous material; 49 U.S.C. § 46312.
4. Aircraft piracy; 49 U.S.C. § 46502.
5. Interference with flight crew members or flight attendants; 49 U.S.C. § 46504.
6. Commission of certain crimes aboard aircraft in flight; 49 U.S.C. § 46506.
7. Carrying a weapon or explosive aboard aircraft; 49 U.S.C. § 46505.
8. Conveying false information and threats; 49 U.S.C. § 46507.
9. Aircraft piracy outside the special aircraft jurisdiction of the United States; 49 U.S.C. § 46502(b).
10. Lighting violations involving transporting controlled substances; 49 U.S.C. § 46315.
11. Unlawful entry into an aircraft or airport area that serves air carriers or foreign air carriers contrary to established security requirements; 49 U.S.C. § 46314.
12. Destruction of an aircraft or aircraft facility; 18 U.S.C. § 32.
13. Murder.
14. Assault with intent to murder.
15. Espionage.
16. Sedition.
17. Kidnapping or hostage taking.
18. Treason.
19. Rape or aggravated sexual abuse.

**Appendix I: Criminal Offenses That Disqualify
Applicants under the Aviation Workers
Program from Acquiring an Airport-Issued
Badge**

20. Unlawful possession, use, sale, distribution, or manufacture of an explosive or weapon.
21. Extortion.
22. Armed or felony unarmed robbery.
23. Distribution of, or intent to distribute, a controlled substance.
24. Felony arson.
25. Felony involving a threat.
26. Felony involving—
 - (i) Willful destruction of property;
 - (ii) Importation or manufacture of a controlled substance;
 - (iii) Burglary;
 - (iv) Theft;
 - (v) Dishonesty, fraud, or misrepresentation;
 - (vi) Possession or distribution of stolen property;
 - (vii) Aggravated assault;
 - (viii) Bribery; or
 - (ix) Illegal possession of a controlled substance punishable by a maximum term of imprisonment of more than 1 year.
27. Violence at international airports; 18 U.S.C. § 37.
28. Conspiracy or attempt to commit any of the criminal acts listed above.

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

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

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<http://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <http://www.gao.gov> and select "E-mail Updates."

Order by Phone

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

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

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

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at www.gao.gov.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Katherine Siggerud, Managing Director, siggerudk@gao.gov, (202) 512-4400, U.S. Government Accountability Office, 441 G Street NW, Room 7125, Washington, DC 20548

Public Affairs

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