# SIDA Airport Security

*February 6, 2018*

Fiscal Year 2017 Report to Congress

Homeland Security

*Transportation Security Administration*

# Message from the Administrator

February 6, 2018

I am pleased to present the following report, "SIDA Airport Security," prepared by the Transportation Security Administration (TSA).

This report was compiled pursuant to Senate Report 114-264 accompanying the Fiscal Year 2017 Department of Homeland Security Appropriations Act (P.L. 115-31). The report "directs TSA to report to the Committee on what steps TSA has already taken to secure our Nation's airports working with airports, relevant State and local law enforcement, and the aviation community."

Pursuant to congressional requirements, this report is being provided to the following Members of Congress:

The Honorable John R. Carter
Chairman, House Appropriations Subcommittee on Homeland Security

The Honorable Lucille Roybal-Allard
Ranking Member, House Appropriations Subcommittee on Homeland Security

The Honorable John Boozman
Chairman, Senate Appropriations Subcommittee on Homeland Security

The Honorable Jon Tester
Ranking Member, Senate Appropriations Subcommittee on Homeland Security

If you have any questions, please do not hesitate to contact me at (571) 227-2801 or the Department's Deputy Chief Financial Officer, Stacy Marcott, at (202) 447-5751.

Sincerely yours,

David P. Pekoske
Administrator

# SIDA Airport Security

## Table of Contents

# I. Legislative Language

This report is submitted pursuant to Senate Report 114-264 accompanying the Fiscal Year (FY) 2017 Department of Homeland Security (DHS) Appropriations Act (P.L. 115-31).

Senate Report 114-264 states:

> The Committee is concerned about the potential for misuse of Secure Identification Display Area (SIDA) badges in the United States stemming from reports that terrorist organizations have used airline workers to carry out attacks in Egypt and Somalia. The Department, in conjunction with airports, airlines, State and local law enforcement, and other agencies as appropriate, shall take actions to secure air travel in the United States, including information-based screening of aviation workers against available domestic and foreign intelligence. The Committee directs TSA to report to the Committee on what steps TSA has already taken to secure our Nation's airports working with airports, relevant State and local law enforcement, and the aviation community. This report should include the number of known cases where SIDA badges were used to bypass secure checkpoints for non-official purposes and the number of cases where individuals who obtained SIDA badges traveled overseas to a foreign terrorist organization.

# II. Background

The Transportation Security Administration's (TSA) mission is to protect the Nation's transportation systems to ensure freedom of movement for people and commerce. TSA's scope includes commercial and general aviation, public transportation, freight and passenger rail, highways, pipelines, and ports. Among these, commercial aviation and the protection of U.S. airports always have been a primary focus because the threat to these modes has been the greatest.

TSA is responsible for securing nearly 440 federalized airports that facilitate upwards of 20,000 domestic flights per day and more than 2,000 outbound international flights per day. U.S. airports are a hub of activity filled with travelers; contractors; airport and airline service workers; federal, state, and local law enforcement officers; and other government employees. As such, significant security challenges persist in the airport setting because of the high number of individuals who need unescorted access to aircraft and secure areas of airports to perform their duties, including Security Identification Display Areas (SIDA).[1] Since the early days of the agency, TSA has focused on the security of SIDAs by requiring vetting of individuals seeking unescorted access to this and other sensitive areas of the airport, and by setting standards for the physical security of SIDAs.

Due in part to reports that terrorist organizations have used aviation sector insiders to carry out attacks, TSA has placed significant emphasis on its Insider Threat Program to deter, detect, and mitigate insider threats to the Nation's transportation sector personnel, operations, information, and critical infrastructure. TSA defines insider threats as individuals with access and/or knowledge that could enable them to exploit vulnerabilities in the transportation system with intent to cause harm, including current and former transportation sector employees, contractors, and partners.

TSA ensures that airport access control is executed properly in partnership with airport and aircraft operators, and other federal agency partners. To fulfill this critical mission, TSA and its stakeholders employ a risk-based security approach that includes:

1. Vetting and credentialing of airport and airline employees prior to being granted unescorted access to secure and sterile areas of the airport;
2. Assessment of vulnerabilities, and development and execution of security programs required by federal regulations;
3. TSA inspections, assessments, and testing of access control systems and airport operations;
4. Unpredictable physical screening/inspections of aviation workers throughout the work day;
5. Aviation worker training, awareness, and education efforts; and
6. Sharing of intelligence and information with partners and stakeholders.

[1] The SIDA is a portion of an airport, specified in the airport's TSA-approved security program, in which certain security measures required by TSA are carried out. See 49 CFR 1540.5.

This approach helps to ensure that resources are applied effectively and efficiently to provide the greatest impact for aviation security, and to reduce the risk associated with insider threat.

# III. Discussion

## A. Existing Measures Securing the Nation's Airports

The aviation security enterprise includes TSA; the Federal Aviation Administration (FAA); other federal, state, local, and tribal government agencies; and private industry stakeholders such as airports, aircraft operators, and cargo supply chain entities. As a community, this enterprise has made progress in addressing the insider threat. Significant challenges remain because of the high number of TSA and non-TSA employees at airports who need unescorted access to aircraft and secure areas of airports to perform job duties. TSA estimates that there are approximately 1.4 million aviation workers with access to SIDAs, which include the secure areas and/or Air Operations Areas (AOA) at U.S. airports as defined in 49 CFR part 1540.

**Aviation Worker Vetting Program**

From its inception in 2001, TSA, in partnership with airport operators, has vetted all individuals applying for unescorted access to the SIDA, and certain other parts of the airport, including cases where the public areas are adjacent to the SIDA. For SIDA access, this vetting has evolved to include a Criminal History Records Check (CHRC) for certain disqualifying criminal offenses; a check for lawful presence in the United States; and a recurrent check against the Terrorist Screening Center's watchlist and other databases. Since 2016, these recurrent checks also include vetting against records of individuals for whom the government lacks reasonable suspicion necessary for watchlisting as a known or suspected terrorist, but who have links or associations with terrorists or terrorist activity. This robust, individually focused vetting covers millions of transportation workers at all TSA-regulated airports. TSA continuously strives to improve individual security threat assessments, and is one of the first federal agencies to implement the Federal Bureau of Investigation's (FBI) "Rap Back" recurrent criminal history vetting service.

**Implementation of the Rap Back Program**

The FBI's Rap Back service provides near real-time notification of new, potentially disqualifying criminal events that enables TSA and airport and aircraft operators to revoke an individual's unescorted access, substantially mitigating the insider threat posed by individuals with disqualifying offenses.[2] TSA's implementation of the Rap Back Program:

- Provides early detection of potentially disqualifying criminal activity, enabling TSA and airport and aircraft operators to vet new information in accordance with TSA regulations;
- Ensures that personal information of aviation workers is protected pursuant to the Privacy Act of 1974, U.S.C. section 552a; and

[2] Examples of disqualifying offenses are: murder, rape, or aggravated sexual abuse; felony arson; and armed or felony unarmed robbery. See 49 USC part 1542.209(d).

- Minimizes direct costs to TSA and stakeholders.[3]

TSA has received considerable interest from airport and aircraft operators to enroll their employees in Rap Back services, particularly following the FBI's elimination of additional Rap Back subscription fees.[4] To further encourage and accelerate Rap Back participation, TSA amended the security directive that required a 2-year CHRC renewal cycle for Rap Back participants by eliminating the biennial, full CHRC renewal cycle for those already enrolled in Rap Back. This change reduces significant administrative burden for the Airport/Aircraft Operator Badging Office (ABO) because the ABO no longer will be required to review the same rap sheet every 2 years if there are no changes. This enables resources to focus on reviewing updates to an individual's criminal history. Thus, Rap Back affords subscribing entities substantial savings in the reduction of CHRC fees related to the full FBI CHRC fee, and resources required to adjudicate criminal history results every 2 years. TSA has collaborated with industry to promote Rap Back service enrollment. The airport[5], aircraft operator, and TSA jointly execute a memorandum of understanding to outline and confirm participation details for entities with SIDA-badged workers.

**Insider Threat Program**

TSA's current Insider Threat Program is developing a holistic enterprisewide preventive approach to mitigating insider risk. TSA's Insider Threat Unit (ITU) serves as the focal point for all insider threat incidents, inquiries, airport/worksite assessments, and education/outreach efforts. The ITU is led by TSA's Office of Law Enforcement/Federal Air Marshal Service, and is supported across the enterprise using the National Insider Threat Task Force "hub" model to coordinate, disseminate, and retain all information when reviewing threat indicators and conducting inquiries and investigations. Reports of insider threat indicators are received from a telephone tip line and email tip address, security policy violations, and internal/external intelligence reports and referrals. To address insider threats, the ITU coordinates inquiries and investigations with the appropriate lead entities to include TSA offices and the DHS Insider Threat Program, as well as federal, state, and local law enforcement; intelligence agencies; and various airport and transit agency/commuter rail law enforcement authorities. The activities highlighted below represent notable multidisciplinary mitigation efforts within TSA.

[3] Prior to October 1, 2016, the FBI's Rap Back subscription costs, separate from the full CHRC, were $2.25 for a 2-year subscription, $6 for a 5-year subscription, and $13 for a lifetime subscription per person; after October 1, 2016, these fees are now $0.

[4] The Rap Back Service is a subscription service offered by the FBI whereby the subscriber is provided with continuous updates to the criminal history of its covered workers. TSA facilitates the establishment and management of Rap Back subscriptions for airports that chose to enroll their SIDA badge holders in Rap Back, and TSA also acts as a conduit from the FBI to the airport for the resulting criminal history updates for affected SIDA badge holders.

[5] Although Rap Back has been implemented fully from a technical perspective, not all airports currently are enrolled because participation is voluntary. As of September 20, 2017, 65 airports are enrolled and an additional 65 have executed a memorandum of understanding with TSA to enable future participation. TSA has focused its outreach efforts on Category X and I airports but is shifting its focus to Category II and III airports for FY 2018.

**Regulatory Compliance Efforts**

TSA conducts inspections to ensure compliance with all TSA regulatory requirements, which include badging/vetting requirements for all TSA-regulated aviation entities and the physical security of the SIDA. Annually, TSA's compliance field offices perform thousands of regulatory inspections, tests, and investigations, as well as assessments, outreaches, and incident management reporting. These compliance activities occur at all airports that operate under a TSA-approved Airport Security Program in accordance with 49 CFR part 1542. TSA also inspects, tests, and assesses domestic aircraft operators and foreign air carriers, cargo supply chain entities, and other aviation stakeholders. TSA takes appropriate enforcement actions when noncompliance is found.

**Airport Self-Vulnerability Assessments**

In 2016, TSA issued Information Circular (IC) 15-01B, recommending that the regulated entities perform detailed and thorough airport insider threat, self-vulnerability assessments. Of the 292 applicable airports operating under complete security programs per regulations, all assessments were completed. Vulnerability assessment areas included: threat intelligence/training; airport access points; identification media vetting and auditing; inspections; and additional measures. The results of these self-vulnerability assessments were analyzed and TSA shared effective measures with aviation stakeholders for their consideration when implementing risk mitigation plans. TSA continues to work with its stakeholders locally to assess airport vulnerabilities through the recommendations made in the IC, ongoing regulatory compliance efforts, and the joint vulnerability assessment process.

**Routine SIDA Audits and Compliance Checks**

TSA long has been sensitive to the need to hold airports, employers, and individuals accountable for the security of identification media, including SIDA badges. TSA's regulations and security programs have required audits of badges, and that workers be rebadged when airports exceed 5 percent of unaccounted for credentials for secure areas, sterile areas, or AOA. In 2016, Congress enacted the FAA Extension, Safety, and Security Act of 2016, which tightened the measures related to airport access control. The Act requires TSA to notify congressional committees of any Category X airport that was missing 3 percent (5 percent for Category I-IV airports) of their SIDA badges. TSA developed a quarterly reporting system to Congress to convey numbers of lost, stolen, or unaccounted for badges for all categories of airports as described above.

Additionally, to enhance airport identification media security, TSA completed three special emphasis inspections (SEI) in each of the first and fourth quarters of FY 2017. These SEIs encompassed identification media audit requirements, reverse identification media audits, and badge deactivation tests.

The Act also directed the Administrator of TSA to develop and implement a metric to measure the security effectiveness of the SIDA that takes into consideration:

- Adherence to access point procedures;
- Proper use of credentials;
- 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;
- Differences in access point characteristics and requirements at airports; and
- Any additional factors that the Administrator considers necessary to measure performance.

TSA determines the effectiveness as follows:

- Obtain the total number of inspections that occurred in the SIDA nationwide per fiscal year;
- Obtain the total number of inspections that were compliant/not compliant for SIDA; and
- Use these numbers to calculate the effectiveness of SIDA nationwide, taking into consideration adherence to access point procedures and proper use of credentials.

This inspection data allow TSA to calculate compliance rates that are used as a proxy for SIDA effectiveness. TSA applies progressive enforcement for noncompliance found during its inspections activities.

In addition, Section 3407 of the FAA Extension Act mandated TSA to develop a model and best practices for unescorted access security that uses intelligence, scientific algorithms, and risk-based factors; ensures integrity, accountability, and control; and subjects airport workers to random physical security inspections conducted by TSA representatives in accordance with the section. In late 2016, in order to meet the requirements of the law, TSA expanded the capability of an already developed risk-based resource deployment model for the public areas of airports, to nonpublic areas. TSA piloted the enhanced model that uses a combination of intelligence, scientific algorithms, data, and local expertise to deploy resources unpredictably to create an expectation of screening for employees at any access point. On the basis of the success of the pilot, TSA plans to deploy the model starting in FY 2018.

## B. SIDA Badge Use for Nonofficial Purposes

In FY 2016, there were 42 instances where an individual used a SIDA badge to bypass secure checkpoints for a nonofficial purpose.[6] None of these instances posed a significant risk to life and safety, and in all cases TSA issued a warning notice or civil penalty. This information is based on data in the Performance and Results Information System, which TSA uses as a repository of information on regulatory inspections, enforcement investigations, and other enforcement activity.

[6] TSA interprets "secure checkpoints" to mean passenger screening checkpoints and has interpreted "nonofficial purpose" as meaning use of the SIDA badge when the individual or employee is off-duty and/or in connection with personal business.

## C. SIDA Badge Links to Foreign Terrorist Organizations

Information relating to any possible travel of current SIDA badge holders overseas for the suspected purpose of joining or engaging with a foreign terrorist organization is available in the attached classified addendum. This addendum will be transmitted to the Committees in a manner pursuant to limitations placed upon sharing of classified information.

In addition, it is important to note that TSA coordinates with U.S. intelligence community and law enforcement partners to ensure the appropriate operational response to mitigate risks identified from credential holders who pose a potential aviation security risk.

# IV. Conclusion

TSA has focused on the security of the SIDA from the early days of the agency. TSA's requirements have evolved with the threat and technological advances. TSA has taken numerous steps to secure our Nation's airports, through working with industry stakeholders, relevant state and local law enforcement, and the aviation community to continue to increase security using a risk-based approach. These continued efforts help TSA to reduce the risk of SIDA badges being used to bypass secure checkpoints for nonofficial purposes. Additionally, the enhancements to the security threat assessment process, such as the implementation of the Rap Back service and vetting of additional terrorism-related records, help to reduce the risk of an insider threat.

# V. Classified Addendum

This information is classified and will be transmitted to the Committees in a manner pursuant to limitations placed upon the sharing of classified information.