February 2017

AMERICA'S AIRPORTS: THE THREAT FROM WITHIN

HOUSE HOMELAND SECURITY COMMITTEE MAJORITY STAFF REPORT

HOMELAND SECURITY
COMMITTEE

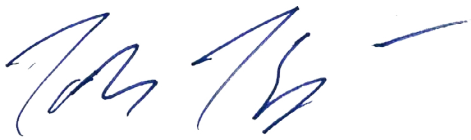
There is a vast network of approximately 450 airports in the United States that are under federal supervision and control. They serve as a critical component of America's economy, connecting people and goods from rural and urban communities across the United States and the world. In 2016, there were over 900 million domestic and international U.S.-bound air passengers, with that number expected to continue to grow significantly on an annual basis for the foreseeable future.

Approximately 900,000 people work at these airports, and many are able to bypass traditional screening requirements that travelers visiting the airports must endure. While the overwhelming majority of these airport workers take the inherent responsibility seriously, there are increasing concerns that insider threats to aviation security are on the rise. Recent insider threat examples discussed in this report include an attempt to detonate a bomb at an airport, gun and drug smuggling, an expressed willingness to smuggle explosives as well as employees who became involved in terrorist activities overseas. In all of these instances, the employees in question had access to secure areas of the airport. These insider threats, and the lack of adequate access controls at airports nationwide, are of particular concern given the rise of terrorist groups bent on penetrating U.S. airport security to commit terrorist acts and "lone wolf" attacks being inspired by terrorist groups like ISIS.

The Subcommittee has worked closely with the Transportation Security Administration (TSA) and the aviation stakeholder community to examine how we can work together to improve access controls and employee screening at our nation's airports. Through hearings, oversight inquiries, site visits and roundtable discussions, the Subcommittee has identified security flaws within our nation's airports and proposed solutions to fix them. The end result included the passage out of the House of multiple bills addressing the insider threat, including H.R. 3102, the *Airport Access Control Security Improvement Act of 2015*, and H.R. 2750, the *Improved Security Vetting for Aviation Workers Act of 2015*.

A number of key legislative provisions from these bills were enacted as part of the *FAA Extension, Safety, and Security Act of 2016*, which was signed into law by President Obama in July 2016. This legislation requires the TSA Administrator to establish a risk-based screening model for employees at airports, enhances the oversight of Secure Identification Display Area (SIDA) issuance procedures, ensures TSA coordinates with interagency watch-listing partners to determine needed Terrorist Identity Datamart Environment (TIDE) category codes for vetting, and requires that TSA issue new guidance for its inspectors to annually conduct a comprehensive review of airport badging office procedures.

However much more needs to be done to improve the state of access controls and mitigate the insider threat facing America's aviation sector. This report makes nine recommendations that will help achieve that goal.



John Katko
Subcommittee Chairman

Table of Contents

I. Introduction

IDENTIFYING THE THREAT

In the months following a series of high profile incidents of aviation workers involved in criminal activity, the Homeland Security Committee's Subcommittee on Transportation and Protective Security (the Subcommittee) launched an extensive, bipartisan investigation into nearly every aspect of airport access controls and employee vetting and screening. Access controls, the capabilities and systems in place to safeguard access to sensitive areas, and the means by which employees are screened at airports were shown to be a source of vulnerability to securing the aviation sector. Through hearings, briefings, stakeholder meetings, legislation, and site visits, the Subcommittee evaluated the aviation community's security capabilities and understanding of the threat environment. We now have introduced a new piece of legislation, the *Aviation Employee Screening and Security Enhancement Act of 2017*, which we believe will significantly assist in mitigating the insider threat.

INCONSISTENT SOLUTIONS TO A CONSISTENT PROBLEM

Inconsistencies exist across the system related to how airport and air carrier security officials educate their credentialed populations on responsibly using their access and reporting suspicious activities. The relationship between stakeholders and local TSA officials varies widely among airports, increasing concern that security gaps are left open by lapses in effective communication and coordination. Similarly, the Subcommittee found that the overall understanding of the threats facing our nation's transportation systems differed greatly among airport officials across the country, leading to the conclusion that many credentialed aviation workers may not understand the potential risk inherent in weak access controls, and TSA can likely do a better job of promoting threat information sharing.

Many credentialed aviation workers may not understand the potential risk inherent in weak access controls.

The sheer diversity among American airports makes security standardization a daunting task. The costs and risks associated with potential disruptions to aviation operations by instituting new security protocols remain a constant worry. Conflict between industry and government stakeholders often impedes needed improvements to aviation security. Furthermore, industry stakeholders are not sufficiently supported in their efforts by their government partners in security. In 2016, TSA partner with airports to conduct vulnerability assessments and implement insider threat mitigation measures. The Subcommittee acknowledges this progress and hopes to see such collaboration continue in the future.

After nearly two years of oversight efforts, the Subcommittee found that the majority of airports do not have full employee screening at secure access points. These airports are unable to demonstrate the security effectiveness of their existing employee screening

efforts, which consist largely of randomized screening by TSA officers or airport law enforcement personnel. There also remains room for improvement on how access to sensitive areas of the airport can be more effectively controlled by airport badging officials. In regard to employee vetting, the Subcommittee uncovered gaps in the types of data collected, as well as the data sets TSA is granted access to by government partners in the Intelligence Community. One airport security official noted that an individual's mandatory ten-year criminal background check could conceivably come back clean, if the person had been serving a prison sentence during that entire ten-year period. Airport authorities articulated concern about their lack of insight into the vetting process conducted by TSA and the FBI. This prevented them from making fully informed decisions when granting badge access to prospective employees. In the midst of multiple and ongoing breaches in airport access controls, the disturbing reality is that it takes just one individual with the right access to cause catastrophic harm.

MITIGATING THE THREAT

The Subcommittee makes the following recommendations to improve the state of access controls and mitigate the insider threat facing America's aviation sector:

1. Airport operators and air carriers should work to better educate aviation workers on their role in mitigating insider threats and securing access to sensitive areas of airports.
2. Airports and TSA should reassess credentialing practices to ensure that individuals with access to secure and sterile areas of airports are held to stringent standards and are regularly reassessed for the risk an individual may pose to aviation security.
3. Airports and air carriers should examine the costs and feasibility of expanding the physical screening of employees.

4. DHS and airports should work to identify advanced technologies for securing employee access and work to further reduce the number of employee access points.
5. TSA should implement the FBI's RapBack Service[1] for all credentialed aviation worker populations in order to more rapidly detect insider threats and leverage the greater resources of DHS and the Intelligence Community to educate its own personnel on the threats facing aviation security and how the agency can better mitigate the insider threat.
6. TSA should identify airports where the relationship between the agency and its stakeholders is in need of improvement and ensure that communication between relevant stakeholders and TSA is both regular and productive.
7. TSA should increase covert testing of Playbook operations at airports across the United States, in order to measure current levels of security effectiveness and provide recommendations to airports and air carriers on how security can be improved. Testing results should be shared with airport operators and air carriers.
8. TSA should strategically target its use of employee screening operations.
9. DHS should be the lead interagency coordinator on insider threats at airports across the United States, through its Homeland Security Investigations (HSI) component, while working with other relevant entities such as the Department of Justice.

No one knows individual airports better than the aviation workers on the ground, and federal regulations must not deter the flexibility of local airports to make the best security choices for themselves. However, recent and ongoing challenges necessitate a holistic and comprehensive assessment of America's airport security posture. This was the approach employed by the Subcommittee throughout the investigation and the lens through which aviation security must be viewed. The Subcommittee hopes that the report will serve as a roadmap for its partners in aviation security to enhance their existing efforts with an ever-vigilant eye on the rapidly evolving threats facing America's transportation systems.

Recent and ongoing challenges necessitate a holistic and comprehensive assessment of America's airport security posture.

II. Evolution and Current State of Airport Access Controls

According to the Government Accountability Office (GAO), TSA officials have long acknowledged the potential threat from airport workers, but deemed the threat a "known and accepted risk."[2] Several years after the attacks of September 11, 2001, TSA conducted only random worker screening at airports throughout the U.S. According to the GAO, when Federal Security Directors (FSDs), the top TSA officials serving in the field at individual airports, voiced their concerns pertaining to insider threats, they were told background checks conducted on airport workers were an adequate safeguard against any potential insider threats. It was not until March 2005 when the Aviation Direct Access Screening Program (ADASP) was implemented that TSA introduced a security screening program for airport employees.[3] The ADASP was designed to detect items such as improvised explosive devises (IEDs), explosives, ammunition, incendiaries, firearms, hazardous materials and suspicious materials or substances.[4]

A key incident, however, that challenged the effectiveness of ADASP occurred on March 5, 2007, when two Comair Airline employees were caught smuggling eight pounds of marijuana and 14 firearms onto a Delta Air Lines commercial airplane located at Orlando International Airport. The plane was bound for Luis Munoz Marin International Airport (SJU) in San Juan, Puerto Rico. Both individuals were arrested and the contraband seized. This incident ultimately prompted Orlando International Airport to adopt 100 percent airport employee screening.[5]

By October 2008, the Department of Homeland Security Office of Inspector General (DHS OIG) determined the implementation of ADASP nationwide had been insufficient and prevented many workers from ultimately being screened. ADASP was shut down in December 2009, shortly after the OIG's report was released and TSA agreed to address the shortfalls of the program.[6] Following the failure of ADASP, TSA implemented various efforts to ensure access control and perimeter airport security including the 2012 *National Strategy for Airport Perimeter and Access Control Security*. Despite these efforts, security incidents involving aviation workers continued to occur.

According to the Government Accountability Office (GAO), TSA officials have long acknowledged the potential threat from airport workers, but deemed the threat a "known and accepted risk."

Not long after the national strategy was adopted, the U.S. experienced its 61st post-9/11 terrorist plot. In December 2013, 58-year-old Terry Lee Loewen of Wichita, Kansas, was arrested and charged with attempting to detonate a vehicle-bomb at Kansas Mid-Continent Airport. Demonstrating the dangers of insider threats, Loewen had worked at the airport as an avionics technician and was able to acquire the necessary wiring materials for the bomb from the airport. Loewen confided to an FBI informant that his badge enabled him to access both the tarmac and terminal, enabling his plot.[7] The FBI was able to detect and disrupt this plot before Loewen posed a serious danger to the traveling public or the airport. As lone-wolf terrorism becomes an increasing threat to domestic security, the U.S. transportation system must prepare for cases such as Loewen's. Over the last five years there have been a number of alarming cases highlighting the threat that aviation workers can pose:

- October 2008: Shirwa Ahmed, an airport cart driver who helped passengers reach their gate, joined al-Shabaab as the first suicide bomber from the U.S. to join the group in Somalia.[8]
- October 2011: Abdisalan Hussein Ali killed himself in a suicide attack at a military checkpoint in Mogadishu. Prior to becoming a terrorist, Ali had worked at the Minneapolis-St. Paul International Airport serving coffee across from Customs and Border Protection personnel.[9]
- November 2014: Three men from Minnesota who had previously worked at Minneapolis-St. Paul International Airport were recruited to fight for ISIS. One individual in particular,

Abdirahmaan Muhumed, had a Secure Identification Display Area (SIDA) badge, granting him access to secure areas of the airport. As an airplane cleaner and employee whose job was to put fuel into airplanes, Muhumed had unlimited access to planes located anywhere on the tarmac. Not only did he have the ability to smuggle a bomb or IED onto the airport's grounds, he also had direct access to any plane that passed through the airport.[10]

- December 2014: Mark Quentin Henry, a Delta Air Lines employee, smuggled a total of 153 firearms, including AK-47 assault weapons, onto 17 Delta flights between Atlanta and New York City in 2014.[11]
- December 2014: Moniteveti Katoa, an aviation contractor at Dallas-Ft. Worth International Airport, bragged to an undercover FBI agent that he could smuggle a bomb onboard an aircraft and offered to fly explosives for a $4,000 fee.[12]
- January 2015: Ernest Abbott, a Federal Aviation Administration inspector was arrested at New York's LaGuardia International Airport after a TSA screener found a firearm in the inspector's carry-on baggage.[13] This inspector had already traveled to New York from Atlanta where he used his SIDA badge to bypass security screening. The inspector flew in the cockpit with the pilots from Atlanta to New York.
- February 2016: In testimony before Congress, TSA states that recent insider threat mitigation efforts have yielded arrests in Dallas, Los Angeles, San Francisco, and Puerto Rico.[14]

In response to security lapses within airports throughout the country, in March 2015, TSA requested the Aviation Security Advisory Committee (ASAC) to review the aviation industry's efforts regarding airport employee screening and ways to address security vulnerabilities. The ASAC made 28 recommendations to help further reduce insider threats posed by aviation employees, including enhanced random employee screening, increased intelligence sharing, security awareness, internal badging office audits and reducing the number of access points to an operational minimum.[15] According to industry representatives, the aviation community is actively working with TSA to implement many of these recommendations.[16]

In April 2015, Homeland Security Secretary, Jeh Johnson, announced an increase in security measures for all employees at airports throughout the U.S., including airline workers. Among the multiple changes was a requirement for those workers holding SIDA badges to undergo fingerprint-based background checks every two years. Additionally, all air carrier and airport workers must undergo TSA screening prior to traveling and random screenings of aviation workers were increased.

Without a comprehensive background check for employees, TSA does not have the ability to screen for those individuals who may harbor ill-will toward the U.S. or have connections to individuals who do.

However, those actions did not address larger problems in the vetting process. In June 2015, the DHS OIG released a report which found that 73 aviation workers who held sensitive jobs within U.S. airports were found to have possible ties to terrorism, which their background checks did not reveal. In addition to these 73 individuals, the investigation concluded that thousands of TSA employee records were incomplete and contained inaccurate information.[17] Without a comprehensive background check for employees, TSA does not have the ability to vet those individuals who may harbor ill-will toward the U.S. or have connections to individuals who do.

Former TSA Administrator Peter Neffenger stated he felt confident that airport employee screening has improved and believes it is more effective than ever during his remarks before a House Homeland Security Committee hearing in May 2016. However, TSA still only checks employee criminal records every two years as opposed to continuous vetting. At the time of writing, only three U.S. airports—Miami International Airport, Orlando International Airport, and Hartsfield Jackson Atlanta International Airport—have implemented full screening of employees and their property before granting access to secure areas of the airport.[18] In addition, TSA is still working with the Federal Bureau of Investigation to deploy recurrent criminal background checks, also known as RapBack, for all SIDA badge holders and vetted populations or employees.

While each airport's vulnerabilities and worker populations are unique, we need to ensure that the overall baseline security framework is robust enough to meet the evolving threat. Our aviation system is interconnected, and we are only as secure as our least secure airport. We must continue this dialogue and ensure that the federal government, airports, air carriers, and the aviation community maintain a continued collaborative focus on this critical issue.

III. Solutions

1. Airport operators and air carriers should work to better educate aviation workers on their role in mitigating insider threats and securing access to sensitive areas of airports.

A majority of aviation security personnel demonstrate leadership and take ownership of securing their respective airports or carriers. However, several site visits and meetings with stakeholders yielded perceptions of complacency or misunderstanding of the threat environment. One such example was when an airport security director could not cite the number of employee access points at their airport—a number that most airport security personnel should be intimately familiar with.

Some stakeholders appeared more intent on placing sole security responsibility—and related costs—on TSA. Additionally, airport operators and air carriers often clash regarding security practices, costs, and protocols—often delaying security improvements and marring cooperation. These inconsistencies in security cooperation and engagement mean that the system as a whole exhibits dangerous points of vulnerability.

2. Airports and TSA should reassess credentialing practices to ensure that individuals with access to secure and sterile areas of airports are held to stringent standards and are regularly reassessed for risk to aviation security.

In recent months, media reporting uncovered that thousands of SIDA badges have gone missing across the United States with concerning gaps of time between when a credential is misplaced and when it is reported missing or deactivated. While many badges also require a pin number or biometric identifier before granting access, these standards vary among airports. Additionally, TSA's inspection and auditing processes have proven to be inadequate. However, airport operators are the ultimate authority on badging and must take responsibility for their credentialing practices.

Relying on self-reporting grants limited visibility to TSA and has led to inconsistencies and discrepancies in both badging regulation interpretation and security practices across the aviation system.

Federal regulation requires that airports issue new badges to the entire SIDA population if more than 5 percent of badges are lost or stolen. Alarmingly, an audit by the DHS OIG, released on October 24, 2016, found that "some airports were misinterpreting guidance on how to determine the acceptable percentage of lost, stolen, or unaccounted for badges; as a result, some airports believed to be in compliance with TSA's security directive had actually exceeded the 5 percent threshold."[19] In response, the OIG recommended that TSA further clarify guidance on its 5 percent threshold and that the agency conduct more special emphasis inspections (SEIs), which delve deeper into auditing practices and results to gain better insight into airport credentialing practices and auditing results.[20]

Relying on self-reporting grants limited visibility to TSA and has led to inconsistencies and discrepancies in both badging regulation interpretation and security practices across the aviation system. Throughout its investigation, DHS OIG auditors found the following examples of lapses in credentialing practices:

- At one airport, 17 former employees were still listed as having active badges.
- Another airport had an employee listed with active credentials almost a year after termination.
- Three former employees at yet another airport were still listed as having active badges.
- DHS OIG auditors alerted an airport operator to an employee's termination by an individual employer at the airport. The airport operator had not been made aware several months after the termination.[21]

Some confusion appears to stem from individual employers within an airport environment failing to update the badging office of employee turnover or termination, meaning that the airport operator was unaware of a need to deactivate the individual's access badge.[22] In some instances, an employee's SIDA credential authorization exceeded the length of time the employee was legally permitted to be working in the United States. Credentials should only be authorized for a period of time commensurate to when an individual is legally permitted to work in the country, and social security numbers should be required to be provided for vetting purposes of U.S. citizens and legal permanent residents.

One airport visited by the Subcommittee articulated a recently-implemented practice by which a random sampling of employee SIDA information is re-vetted monthly, in order to provide better insight into potential security risks between biannual background checks. Other airports have also developed penalties for employees who fail to report misplaced credentials in a timely manner or who continually lose security credentials.

Credentialing responsibility also lies with TSA, since the agency provides a general thumbs-up or down based on a Security Threat Assessment (STA) of an employee's credential application provided by airports to TSA for vetting and analysis. According to the OIG's report on SIDA badge management, TSA could mitigate the risk of unauthorized access to secure and sterile areas of airports by spreading best practices used by some airports to keep track of SIDA credentials.

3. Airports and air carriers should examine the costs and feasibility of providing expanded employee screening.

Most airport operators and air carriers have strongly opposed moving towards full employee screening. With the exception of three airports that have implemented full employee screening, the vast majority of airports maintain that randomized, targeted employee screening by TSA and airport law enforcement is a more effective deterrent to insider threats, as it is less predictable and prone to defeat from bad actors who would otherwise devise a work-around for criminal or terrorist activity. Moreover, stakeholders argue that there is not an agreed-upon industry definition of what constitutes 100 percent, or full employee screening, due to the great variations in uses of technology, credentials,

and personnel across the country. The challenge in making sweeping nationwide security requirements is that each of the more than 450 federalized airports in the United States is unique.

Over the course of the Subcommittee's investigation, one airport exemplified an effective randomized screening practice. The security director enhanced TSA screening operations by utilizing the airport's own law enforcement resources to set up targeted screening at randomized access points at different times. Rather than concentrating on screening a large number of employees, which is an issue with TSA employee screening, airport law enforcement focused on randomization and unpredictability. This approach is the best implementation of randomized employee screening the Subcommittee has observed, to date.

While previous assessments of the costs and feasibility of full employee screening have been conducted by the DHS OIG, they have focused on a scenario in which TSA conducts employee screening. There is a gap in available data which fully assesses the cost and feasibility of full employee screening. Until such data exists, a legitimate best course of action cannot be determined. Even though a number of commercially successful airports and carriers have implemented full employee screening, industry stakeholders remain largely opposed to conducting cost and feasibility assessments. Despite expressed opposition to full employee screening, airport operators, air carriers, and TSA have not presented any substantive data demonstrating that full employee screening would be cost prohibitive and would not meaningfully enhance security. Two major airports visited by the Subcommittee have implemented robust full employee screening, each with programmatic annual operating costs of less than $3.5 million. While costs would certainly vary among airports depending upon size, volume, and screening methods, cost-sharing agreements between airport operators, airlines, and TSA could make such screening a reality.

In response to a number of security incidents involving its own employees, one air carrier began conducting a version of full employee screening at a number of airports across the country where the carrier has extensive operations. With proliferating threats to aviation security, the concept should not be dismissed outright, particularly when noting that many airports overseas already have implemented full employee screening. It is very possible that targeted, randomized screening does provide an adequate security deterrent, when correctly implemented; however, all options for enhancing airports' security posture and mitigating insider threats should be thoroughly considered.

4. Airports should work to identify advanced technologies for securing employee access and work to further reduce the number of employee access points to an operational minimum.

Airports vary greatly in their use of biometric solutions, number of employee access portals, as well as which security measures are in place at employee access portals. Biometrics, using either fingerprints or retina identification to match the SIDA badge being swiped for access, add an additional layer of security to airport access controls. While there still exists an insider threat posed by an individual using his or her own SIDA badge for nefarious

purposes, it would at least partially stem potential problems from the hundreds of badges that go missing each year.

5. TSA should implement the FBI's RapBack Service for all credentialed aviation worker populations in order to more rapidly detect insider threats and leverage greater resources of DHS and the Intelligence Community to educate its own personnel on the threats facing aviation security and how the agency can better mitigate the insider threat.

The FBI's Rap Back Service provides 24/7 vetting of credentialed populations, and would give TSA, airport operators, and air carriers significantly better insight into instances of arrest, arraignment, prosecution and other circumstances which could potentially disqualify an employee from maintaining their secure area access. Currently, employees are expected to self-report disqualifying offenses which occur during the period of time between background checks, which are legally required every two years. Therefore, in many instances, an employee may be able to maintain his or her secure access even after being arrested or charged with a disqualifying offense until the next time he or she is required to undergo a background check. RapBack would significantly improve this security gap by making such vetting perpetual. While technical challenges have delayed use of RapBack, TSA employees are now included in the program, and several airports and air carriers have begun working with TSA to implement the service among their credentialed populations.

In 2015, a DHS OIG report found that 73 aviation workers with links to terrorism were either currently or recently employed at airports across the United States with access to secure and sterile areas.[23] Subsequent oversight efforts revealed that while TSA reviewed each individual and determined whether they were a threat to aviation security, the agency had missed terrorist ties due to a lack of access to certain data sets held by other entities within the U.S. Government. Despite longstanding efforts to be granted access to additional intelligence databases, DHS and TSA were met with resistance and delay by other federal agencies.

After media and Congressional pressure, TSA was granted additional access by the Office of the Director of National Intelligence, though some officials within TSA have admitted that more is needed in order to provide sufficiently robust vetting to aviation workers. TSA has dispatched Field Intelligence Officers to educate personnel on the importance of catching prohibited items and conducting proper screening of passengers at the security screening checkpoint; however, the Subcommittee has not been made aware of any efforts to bolster agency employee screening operations by informing TSA screeners of the scope and seriousness of the insider threat.

TSA should work to better educate their screening personnel on the insider threat they are seeking to mitigate. Such an effort should also involve joint briefings and collaboration with federal, state, and local agencies represented at the airport. While TSA personnel's mission is to screen solely for security threats, an understanding of what fellow DHS components, such as Customs and Border Protection (CBP) and Immigration and Citizenship

Enforcement (ICE), along with efforts of the FBI and local law enforcement would help give screeners context of the totality of the threat facing airports and why their security function is critical. The need for information-sharing and security collaboration was a primary lesson learned after the terror attacks of September 11, 2001. Government and industry partners in aviation security would be wise to better facilitate a post-9/11 model and mindset within the aviation sector.

6. TSA should identify airports where the relationship between the agency and its stakeholders is in need of improvement and work to ensure that communication between relevant stakeholders and TSA is both regular and productive.

Like many professional interactions, the security of our nation's critical transportation systems is directly tied to the health and wellbeing of the relationships between aviation stakeholders and TSA. Over the course of its existence, TSA has often struggled to maintain positive working relationships between its local personnel and the airport communities in which they operate. Breakdowns in this relationship can contribute to a lack of information exchange and security cooperation, resulting in security failure and unnecessary risk.

TSA should ensure that its own personnel are empowered to work closely with airline representatives, airport operators, employee unions, and local law enforcement to cater operations to the specific security needs of individual airports. Similarly, airports and air carriers should be proactive in engaging and working with TSA at the local and federal level. The unique makeup of American aviation security, which is heavily federalized, presents challenges when compared to most aviation security arrangements across the globe, particularly at the local level. As both regulator and operator, TSA must manage its relationship with its stakeholders from a position of respect and mutual cooperation, while maintaining the authority to provide the security needed to protect the traveling public and critical infrastructure.

During the summer of 2016, substantial wait times at airports nationwide prompted TSA and airports to enhance their levels of cooperation. With industry support, TSA stood up a national incident command center and instituted local coordination meetings. The Subcommittee hopes to see such collaboration replicated in relation to access controls.

7. TSA should increase covert testing of playbook operations at airports across the United States, in order to measure current levels of security effectiveness and provide recommendations to airports and air carriers on how security can be improved. Covert testing results should be shared with airport operators and air carriers.

In June 2015, results of covert testing by the DHS Inspector General were leaked to the media showing that TSA screeners exhibited a 95 percent failure rate in screening passengers for prohibited items at the checkpoint. Such dismal results set off a wave of Congressional and public scrutiny, which led to aggressive retraining and optimization efforts by newly-appointed Administrator Neffenger. The covert testing, known as "red team" testing, unveiled significant security vulnerabilities and mismanagement issues within the agency, and has resulted in a number of reforms to better screen passengers.

The Subcommittee believes that covert testing should be conducted on TSA's employee screening operations in order to determine the security effectiveness of screening and provide insight into how it can be improved. Should such testing occur, the results and recommendations for improvements should be shared with airport operators and air carriers, in order to give them a glimpse into how their SIDA population is being screened and what vulnerabilities may exist.

8. TSA should target its use of employee screening to be more strategic.

In the wake of the Atlanta gun smuggling incident, Secretary Johnson directed TSA to ramp up its use of Playbook operations conducted by TSA personnel related to employee screening operations conducted by TSA personnel. However, there has been no data revealed to the Subcommittee that such screening—in its current form—is effective. After observing TSA's Playbook operations at two different airports, there are concerns that TSA personnel are more focused on screening large numbers of employees, rather than focusing on effectiveness, deterrence, and unpredictability. Generally speaking, TSA Playbook operations are conducted at highly trafficked employee access points, which can be easily avoided by an employee seeking to circumvent screening. TSA maintains that Behavior Detection Officers, as well as law enforcement partners, assist in watching for individuals seeking to avoid screening when a Playbook operation is being conducted. Despite this, the patterns and practices of such screening can easily become predictable. TSA should undertake a comprehensive effort to make Playbook operations related to the screening of airport and air carrier employees measurably effective, targeted, and strategic. Without improvements to the status quo, TSA, airports, and air carriers will not achieve the desired effect of creating an expectation of screening among the credentialed employee population.

9. DHS should be the lead interagency coordinator on insider threats at airports across the United States, while working with other relevant entities, like the Department of Justice.

DHS is the appropriate federal entity to lead interagency coordination efforts in the airport environment. The Subcommittee has received numerous briefings and observed efforts of TSA, ICE, CBP, and the FBI to mitigate criminal and terrorist plots across the U.S. aviation system, and is convinced that DHS components have the best resources and capabilities for effectively securing airports and passengers.

Redundant efforts led by the FBI have, indeed, led to a number of important investigations, arrests, and even convictions of aviation workers. However, in its operations, the FBI does not adequately leverage the resources of its DHS counterparts, which could lead to more effective threat mitigation. Moreover, the Subcommittee is concerned that the FBI is not notifying other relevant agencies in a timely manner and should better leverage the expertise of partner agencies. The FBI has not been forthcoming to Congressional requests for information on threats to aviation—a matter entirely within the jurisdiction of the Homeland Security Committee.

In stark contrast, ICE's Homeland Security Investigations (HSI) division has provided productive and proactive insight to the Subcommittee on its years of investment and experience in fine-tuning its own airport investigative task forces and works more diligently with partner agencies. HSI has developed unparalleled inroads in the aviation security community and well-rooted relations with both airport and air carrier stakeholders. For this reason, the Subcommittee believes that the FBI should take steps to combine airport task force efforts under the leadership of the DHS.

IV. Progress Made

During the course of this investigation, the Subcommittee visited 18 airports of varying size, geographic location, and security standards to gauge overall efforts aimed at improving access controls and mitigating the insider threat to aviation. The visits demonstrated a more coordinated, engaged aviation security community than had been witnessed in the past. The Subcommittee also noted the effective implementation of a number of security recommendations put forth by the Aviation Security Advisory Committee, in its final report on the matter issued on April 8, 2015.[24] Throughout the Subcommittee's investigation, one thing was consistent—federal, state and local government personnel, law enforcement, and aviation stakeholders are steadfastly committed to a secure transportation system. The gaps and vulnerabilities observed are not a condemnation of existing efforts, but are rather intended to augment those efforts and identify areas in which further improvements can be made.

For its part, TSA has attempted to implement policies and initiatives to bolster security and reduce access control vulnerabilities. Testifying before Congress in February 2016, Darby LaJoye, TSA's Assistant Administrator for Security Operations, discussed the agency's role in airport access controls, including aviation worker credentialing. He stated that TSA implemented multiple measures intended to enhance efforts to combat insider threat vulnerabilities. These included requiring airlines and airports to conduct fingerprint-based criminal history records checks every two years for every badge holder until an automated vetting process has been implemented; a reduction in total number of access points leading to a secure area of an airport; and an increase in employee random screening.[25]

TSA's efforts to address insider threats at U.S. airports have shown encouraging results. From 2014 to 2015, TSA increased the total number of physical employee screenings from 2.1 million to 12.9 million and 88 percent of domestic airports have reduced their total number of access points. This has resulted in the elimination of approximately 500 access points throughout the country. Additionally, TSA's Insider Threat Unit, housed within the agency's Office of Law Enforcement, continues to collaborate with both state and federal partners to actively monitor criminal activity within airports. According to TSA, these efforts have led to several arrests including those in Dallas, Los Angeles, San Francisco, and Puerto Rico.[26] One of the major improvements seen at TSA in recent months is enhanced access to terror-related data held by the FBI. Since 2012, the federal government, airport authorities, airlines, aviation community stakeholders, and Congress have all taken steps to improve both the vetting and physical screening of aviation workers. However, many of these steps have been reactionary, and implemented on an ad hoc basis.

The Subcommittee did observe many examples in which access points have been reduced, new perimeter security and badging enhancements have been implemented, and airport operators and air carriers have gone above and beyond minimum required security standards. One airport has even developed behavior detection training for its employees, as well as an insider threat mitigation strategy. At least two major air carriers have also taken proactive steps to enhance the screening operations of both employees and passengers at major hub airports, and TSA has begun to engage airports and air carriers on a more consistent basis. These efforts are encouraging and airports and air carriers should continue to implement enhanced security procedures that best suit their individual operating environments. The vast majority of airports visited by the Subcommittee referenced improved communication and relationship-building efforts on the part of TSA and many enjoy productive working relationships with their local TSA Federal Security Directors.

V. Conclusion

During initial oversight efforts following the Atlanta weapons trafficking incidents, the aviation community appeared to be disturbingly disengaged from the threat posed by bad actors inside an airport's secure areas. However, in the course of its investigation, the Subcommittee witnessed progress made by airports and air carriers responding to the heightened threat environment, media, TSA, Congressional scrutiny, and ASAC recommendations.

The findings and recommendations of the investigation show that a great deal of progress is still needed and that America's airports and aircraft remain vulnerable to attack and exploitation by nefarious individuals. While much work has been done, the Subcommittee remains concerned that adequate awareness does not exist system-wide and has yet to trickle down from corporate security officers, TSA, and law enforcement to the frontline workforce where vulnerabilities are most-often exploited.

Recently enacted legislation should continue the progress already being made to provide greater oversight to SIDA access procedures and access control enhancements; although Congress, TSA, and stakeholders have failed to go far enough in addressing perimeter security concerns, employee screening, and the overall state of security vetting before individuals are granted access to sensitive areas of airports.

Moreover, the vulnerabilities shown by recent incidents at both domestic and foreign airports demonstrate the troubling reality that current security standards would likely fail to prevent a determined adversary with insider access from causing harm to an airport or aircraft. Industry infighting, jurisdictional battles, inconvenience, and cost concerns are not justifiable reasons to cause delays to enhancing the security of the American homeland and our aviation system. America's aviation sector is the envy of the world, and partners in aviation security should be in a constant state of vigilance against risks to its security and strength.

Appendix I: Committee Activities

LEGISLATION

H.R. 2750 – Improved Security Vetting for Aviation Workers Act of 2015

H.R. 3102 – Airport Access Control Security Improvement Act of 2015

H.R. 5056 – Airport Perimeter and Access Control Act of 2016

RELEVANT SUBCOMMITTEE HEARINGS

"*A Review of Access Control Measures at Our Nation's Airports.*"
February 3, 2015. (Serial No. 114–1)

"*A Review of Access Control Measures at Our Nation's Airports: Part II.*"
April 30, 2015. (Serial No. 114–1)

"*How TSA Can Improve Aviation Worker Vetting*."
June 16, 2015. (Serial No. 114–21)

Field hearing in Syracuse, NY, "*Examining Critical Security Measures, Communications, and Response at Our Nation's Airports.*"
October 6, 2015. (Serial No. 114–39)

OTHER OVERSIGHT ACTIVITIES OF THE SUBCOMMITTEE

- During the course of the last two years, the Subcommittee has consulted with representatives from TSA, DHS Office of Inspector General, Government Accountability Office (GAO), American Association of Airport Executives (AAAE), Airports Council International (ACI-NA), Airlines for America (A4A), Delta Airlines, JetBlue Airlines, American Airlines, United Airlines, U.S. Travel Association, Global Business Travel Alliance, Cargo Airline Association, Transportation Trades Department (AFL-CIO), Southwest Airlines Pilots Association, Association of Flight Attendants (CWA), Air Line Pilots Association, and the American Federation of Government Employees (AFGE) to discuss airport access controls.
- On June 9, 2015, the Chairs of the Full Committee, the Subcommittee on Transportation Security, and the Subcommittee on Oversight and Management Efficiency, sent a letter to the Secretary of Homeland Security regarding the Inspector General's report TSA Can Improve Aviation Worker Vetting (OIG-15-98) which found that 73 aviation workers with access to secure areas of airports across the United States were found to have ties to terrorism.
- From October 2015 to August 2016, Subcommittee staff conducted site visits to multiple airports in various regions in the United States to investigate employee access controls and insider threat prevention and mitigation efforts.

- On December 16, 2015, Chair of the Subcommittee on Transportation Security sent a letter to the Administrator, Transportation Security Administration, regarding the state of airport access controls across the United States.
- On June 6, 2016, the Chair of the Committee sent a letter to the Secretary of Homeland Security, regarding recent news reports that a Somali man accused of war crimes, was working as a security guard at Dulles International Airport.

Endnotes

1 The RapBack service allows authorized agencies to receive notification of activity on individuals who hold positions of trust (e.g. school teachers, daycare workers) or who are under criminal justice supervision or investigation, thus eliminating the need for repeated background checks on a person from the same applicant agency to identify persons arrested and prosecuted for crimes, Rap Back provides a nationwide notice to both criminal justice and noncriminal justice authorities regarding subsequent actions. Retrieved from: FBI, "Next Generation Identification," at https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/ngi

2 Government Accountability Office. (2009). "A national strategy and other actions would strengthen TSA's efforts to secure commercial airport perimeters and access controls". (GAO Publication No. 09-399). Washington, D.C.: U.S. Government Printing Office.

3 Ibid.

4 Federal Aviation Administration, "Aviation Direct Access Screening Underway," at http://www.tc.faa.gov/act4/insidethefence/2006/1012_18_directscreening.htm

5 Department of Homeland Security Office of the Inspector General. (2008). "TSA's security screening procedures for employees at Orlando International Airport and the Feasibility of 100 percent employee screening". (OIG Publication No. 09-05). Washington, D.C.: U.S. Government Printing Office.

6 Government Accountability Office. (2009). "A national strategy and other actions would strengthen TSA's efforts to secure commercial airport perimeters and access controls". (GAO Publication No. 09-399). Washington, D.C.: U.S. Government Printing Office.

7 Lucaccioni, Cassandra. (2013, December 15). "61st terrorist plot against the U.S.: Terry Lee Loewen plot to attack Wichita Airport". The Heritage Foundation. http://www.heritage.org/research/reports/2013/12/terry-lee-loewen-terrorist-plot-in-wichita-kansas-airport

8 David Johnson, "Militants Drew Recruit in U.S., F.B.I. Says." The New York Times. 23 February 2009. http://www.nytimes.com/2009/02/24/washington/24fbi.html

9 Josh Kron, "American Identified as Bomber in Attack on African Union in Somalia." The New York Times. 30 October 2011. http://www.nytimes.com/2011/10/31/world/africa/shabab-identify-american-as-bomber-in-somalia-attack.html

10 Lyden, Tom. (2014, November 17)"Insider threat: Side-by-side with a future terrorist at Minneapolis-St. Paul International Airport" Retrieved from http://www.fox9.com/fox-9-mn-special-archive/1642467-story

11 David Beasley, "Atlanta baggage handler charged with helping smuggle guns onto flight." Reuters. 23 December 2014. http://www.reuters.com/article/us-usa-georgia-state-crime-guns-idUSKBN0K11FD20141223

12 Kevin Krause, "Ringleader of Group That Wanted to Smuggle Drugs Through DFW Airport Gets 15 Years." Dallas News. 22 September 2016. http://www.dallasnews.com/news/crime/2016/09/22/ringleader-group-wanted-smuggle-drugs-dfw-airport-gets-15-years

13 "FAA Inspector Charged with Bypassing Atlanta Airport Security Requirements." Department of Transportation Office of Inspector General Release. 24 April 2015. https://www.oig.dot.gov/library-item/32468

14 Deputy Assistant Administrator, Transportation Security Administration. 114th Congress, Second Session. (2016, February 3) (Testimony received by the committee from Darby LaJoye).

15 "TSA adding security measures, including more frequent background checks, for aviation workers". (2015, April 20). Retrieved from http://www.foxbusiness.com/markets/2015/04/20/tsa-adding-security-measures-including-more-frequent-background-checks-for.html

16 Ibid.

17 Ibid.

18 Pegues, Jeff. (May 25, 2016) "TSA blasted for insider threat security gap." Retrieved from http://www.cbsnews.com/news/tsa-blasted-for-insider-threat-security-gap/

19 Department of Homeland Security Office of the Inspector General (2016, October 14). "TSA Could Improve Its Oversight of Airport Controls over Access Media Badges". (OIG Publication No. 17-04).

20 Department of Homeland Security Office of the Inspector General (2016, October 14). "TSA Coul d Improve Its Oversight of Airport Controls over Access Media Badges". (OIG Publication No. 17-04).

21 Department of Homeland Security Office of the Inspector General (2016, October 14). "TSA Could Improve Its Oversight of Airport Controls over Access Media Badges". (OIG Publication No. 17-04).

22 Department of Homeland Security Office of the Inspector General (2016, October 14). "TSA Could Improve Its Oversight of Airport Controls over Access Media Badges". (OIG Publication No. 17-04).

23 Department of Homeland Security Office of the Inspector General (2015, June 4). "TSA Can Improve Aviation Worker Vetting". (OIG Publication No. 15-98).

24 The Aviation Security Advisory Committee's final report included a number of recommendations relating to how airport access controls may be improved across the aviation system. The report examined issues such as employee vetting and screening, disqualifying offenses for airport employees, and the role of the Transportation Security Administration.

25 Deputy Assistant Administrator, Transportation Security Administration. 114th Congress, Second Session. (2016, February 3) (Testimony received by the committee from Darby LaJoye).

26 Ibid.