ASAC
AVIATION SECURITY ADVISORY COMMITTEE

April 8, 2015

Mr. Melvin Carraway
Acting Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Acting Administrator Carraway:

The Aviation Security Advisory Committee (ASAC), based on the work of our Working Group (WG) on Airport Access Control, is pleased to submit its Final Report with respect to an evaluation of options for improving airport employee access control.

By letter of January 8, 2015 to the ASAC, you requested assistance with reevaluating airport employee screening in light of the discovery of an alleged weapons smuggling operation at a major airport that used passenger airliners to transport the contraband. In response to the serious concerns which this finding raised about aviation security, the ASAC created a WG tasked with analyzing the adequacy of existing security measures and recommending such additional measures as may be needed to improve employee access controls. The WG, which is comprised of a broad cross section of industry experts, was supported by representatives of TSA and the Homeland Security Studies and Analysis Institute (HSSAI). I think it is important to recognize the work of these individuals who have spent the last 90 days deeply involved in this issue. A list of the participants is included in the Report. Of special note is the work of Ken Dunlap (IATA), ASAC's Vice Chair, who volunteered to lead the effort and has spent most of the last 90 days totally engrossed in this project and Jerry Wright (ALPA) who acted as our "Editor-in-Chief" in the actual drafting of the Report.

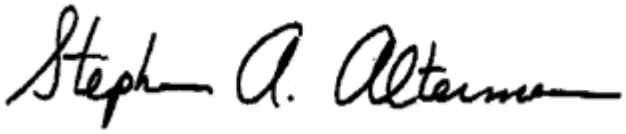
The WG held its first meeting on February 2, 2015, and has met eight additional times in the completion of this 90-day study. Status reports were provided at the 30 and 60-day points of the WG's deliberations that provided information on the areas of analysis and direction of the group with respect to its tasking. The WG was aided in its work by numerous government and industry subject matter experts who briefed the body on various related aspects of employee access control. The WG's report and proposed recommendations were presented to a plenary meeting of the ASAC on April 3, 2015 and were unanimously approved.

The WG took the opportunity afforded by its tasking to analyze a broad range of airport employee access issues, not just those associated with smuggling contraband. The recommendations provided in the final report reflect the Group's belief that reasonable and effective measures, tailored to the unique circumstances at each individual airport, can and should be taken to protect against potential acts of terrorism and criminality. If

TSA determines that implementation of any or all of the recommendations in the report are appropriate, recognizing that not all stakeholders are represented on the WG, ASAC also strongly recommends that, absent specific, credible threat information, any future regulatory actions should be made through the notice and comment process that affords affected stakeholders the opportunity to provide input.

On behalf of the ASAC, it has been our pleasure to assist the TSA and the aviation community through participation in this endeavor. We appreciate the professionalism, collaboration, and support of the TSA and HSSAI in this effort. The WG stands ready to answer questions about the report and/or provide additional assistance to you as needed.

Sincerely,



Stephen A. Alterman
Chairman
Aviation Security Advisory Committee

Attachment

FINAL REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE'S WORKING GROUP ON AIRPORT ACCESS CONTROL

Executive Summary

On January 8, 2015, the Transportation Security Administration's (TSA's) Acting Administrator asked the Aviation Security Advisory Committee (ASAC) to identify new security measures for industry employees to address potential vulnerabilities related to the sterile areas of US airports. The catalyst for this request was the news that an employee gun-smuggling ring had been uncovered at the Hartsfield-Jackson Atlanta International Airport. The ASAC convened a broad cross section of leading experts from airports, airlines, law enforcement, labor, and airport users to create the Working Group on Airport Access and Control (the WG) for the purposes of this tasking.

The WG was given 90 days to study how vulnerabilities are addressed through existing TSA security programs, industry best practices, methods of employee screening within and outside the US, and visit a few US airports. The WG developed recommendations to address concerns prompted by the discovery of a gun smuggling ring operating, but they also go well beyond that concern.

At the beginning of this process, the WG explored the practicality of performing 100 percent physical screening of employees, which was called for by some in the wake of the gun-smuggling incident. The WG concluded that such a measure would not be a "silver bullet" solution and that there were other, more effective and less costly methods of securing the sterile areas of airports.

The WG also concluded that the provision of so-called "100 percent measures" as a layer of airport security does not appreciably increase the overall level of system-wide protection, nor does it lower over-all risk. In this context, the WG agreed with the congressionally mandated report of the 2008 Homeland Security Studies and Analysis Institute's (HSSAI's) report titled, "Airport Employee Screening Pilot Program Analysis," which concluded that "a random screening strategy is the more cost-effective solution" for airports.

The ASAC's recommendations were developed within the context of Risk-Based Security (RBS), a holistic approach to aviation security endorsed throughout every level of the Department of Homeland Security (DHS). This approach acknowledges the globally interconnected aspects of the US air transport system, the varied infrastructures supporting it, the availability of robust employee pre-screening systems, and the need to apply finite aviation security resources efficiently and effectively. The recommendations also acknowledge the view that there are significant differences in the threats posed by criminal activity and terrorism and that the risks and proposed mitigation efforts must recognize this difference.

The WG used an analytical model that followed the flow of typical airport employment and credentialing practices, i.e., pre-employment vetting, badging, arriving at work and entering secure areas, performing daily activities, and leaving work. The

WG segmented the model into five areas of analysis and generated recommendations in each of them, as follows:

- Security Screening and Inspection
- Vetting of Employees and Security Threat Assessment
- Internal Controls and Auditing of Airport-Issued Credentials
- Risk-Based Security for Higher Risk Populations and Intelligence
- Security Awareness and Vigilance

These recommendations focus on activities under the jurisdiction of the TSA granted to it under the Aviation and Transportation Security Act (ATSA, Public Law 107–71 November 19, 2001). The WG fully expects that these recommendations will concurrently mitigate criminal activity in the secured and sterile areas of airports as well. The 28 recommendations address issues requiring varying degrees of support from Congress and the DHS. The recommendations are, to a large extent, interdependent and do not stand alone, which makes prioritization difficult. Due to the complexity and the number of associated variables in this regard, the WG did not have the time to prioritize the recommendations, but would be pleased to discuss this matter further.

The TSA has provided the WG with a high-level cost categorization of certain recommendations. Due to time constraints, the WG was not able to evaluate this analysis. The WG encourages further cost analysis be performed in follow-up. The WG has also identified areas where additional study may be warranted.

The WG strongly urges the TSA's future actions in regard to employee screening and access control to be informed by these community-driven recommendations, and that the unique differences between airport and airline necessitates a risk-based approach. Any actions taken by TSA, absent specific, credible threat information, should be made through the notice and comment process which affords stakeholders the opportunity to provide input.

The following high-level summary of the recommendation areas of this report is offered by the ASAC as a survey of its work.

Security Screening and Inspection

- TSA, with associated industry support, should increase the frequency of random and unpredictable employee screening/inspection at airports. Each employee should arrive at work with the expectation that he or she will be subject to random screening/inspection during his or her work day.

Vetting of Employees and Security Threat Assessment

- Employee vetting should be strengthened by updating the list of disqualifying criminal offenses, instituting continuous criminal activity monitoring through the inclusion of additional Federal Bureau of Investigation (FBI) and DHS data sources, and maintaining a national database of airport employees whose credentials have been revoked for cause. The addition of training programs to these measures will provide a more comprehensive, and in some cases a real-time, ability to assess airport employee access privileges.

Internal Controls and Auditing of Airport-Issued Credentials

- TSA and industry should strengthen policies and penalties associated with accountability and control of airport identification media (i.e., cards/badges/seals). This should include further restricting access privileges, access points, enhancing auditing practices for issued badges, and expanding use of CCTV systems to monitor employees at certain entry points and other areas.

RBS for Higher Risk Populations and Intelligence

- TSA should expand domestic intelligence collection, analysis, and communication with the aim of providing actionable measures that can be employed during employee screening/inspection. This should include social media monitoring with traditional intelligence sources. Concurrently, TSA should work with industry to improve private/public intelligence dissemination through existing and emerging sharing platforms and employee training.

Security Awareness and Vigilance

- Industry security awareness programs should be strengthened through the inclusion of TSA, FBI and US Customs and Border Protection data on key indicators of insider threat and suspicious activity. In conjunction, better use and sharing of airport security assessment results needs to be incorporated into the FBI-TSA-industry partnership. TSA and industry should expand and promote local and national reward programs to encourage employees to report security concerns.

The ASAC would like to thank TSA Acting Administrator Carraway and his staff for fully supporting the work of this group. We would also like to acknowledge the role of the HSSAI for providing data and expertise that strengthened many of our recommendations.

Table of Contents

Introduction

Good security begins with good people who can be trusted to perform their jobs and responsibilities in a manner that poses no threat of intentional harm to themselves or others. This is so because the most expensive, complex, and sophisticated security systems may be defeated by individuals with the insider knowledge, motivation and determination to cause harm to persons and property. Accordingly, individuals who are hired to perform work in the commercial aviation domain must be held to a very high standard of integrity, and their trustworthiness should be assessed on an ongoing basis during the time of their employment, not just as an initial condition of hiring.

In late December 2014, it was reported that several individuals involved in an alleged gun-smuggling ring had been arrested for using commercial airliners to transport prohibited items from the Hartsfield-Jackson Atlanta International Airport to New York area airports. This news understandably created considerable anxiety for the general public, government and industry. In response to this security breach, the Acting TSA Administrator asked the Aviation Security Advisory Committee (ASAC) in January 2015 to establish a Working Group on Airport Access Control (the WG).

The WG was created with a cross section of airport, airline and labor representatives to "provide a forum and procedures for the aviation community to develop a report to the TSA on current and any innovative methods for vetting and physical screening of individuals entering the secure area of an airport." The WG was given the latitude to consider "a number of Risk-Based Security (RBS) options related to airport access control, including policy and procedures, industry best practices, technology, and employee training."

The WG was comprised of 24 individuals (reference Appendix 3) from a wide variety of aviation security, law enforcement and other security related backgrounds. Seven senior executives from the TSA and the HSSAI supported the WG. The deliberations of the WG were enhanced by briefings from subject matter experts and a review of pertinent studies on the subject of employee access controls (reference Appendix 1). The WG began meeting February 2, 2015 and met on eight different days concluding its deliberations on March 31, 2015. Several conference calls also supplemented the in-person meetings. Deliverables were due to TSA on February 7 (30-day report) and March 9 (60-day report), with the final report due on April 8. The WG presented its report to the full ASAC on April 3, 2015 and it was considered and unanimously adopted by that group without amendment.

The WG focused on the types of screening regimens that would best address an insider threat posed by terrorists at our nations' airports. It is essential that the reader recognize that criminal actors differ substantially from would-be terrorists in their motivation, modus operandi, pre-event planning process, behaviors, and sheer numbers.

The comprehensive recommendations put forth in this document are meant to prevent terrorist attacks within the secure areas of airports. An ancillary benefit will be the discovery of some criminal enterprises but neither these nor any strategies will completely eliminate the criminal element. That said, the WG believes that improvements can and should be made to mitigate against the potential for all types of criminal activity to include gun smuggling and other forms of illicit and potentially dangerous behavior in our nation's aviation system.

Risk-Based Security

During its first decade of existence, TSA employed a one-size-fits-all method to aviation security while building a layered security system and deploying more capable technologies. Beginning in October 2011, TSA began to implement Risk-Based Security (RBS) procedures for security screening/inspection of employees, passengers and their accessible property. Under the current passenger-centric RBS approach, TSA conducts pre-screening to differentiate passengers by risk and affords expedited physical screening to passengers assessed as lower risk. RBS increases operational efficiency and security effectiveness by allowing TSA to focus fewer resources on lower risk travelers and more on higher risk passengers, or those about whom less is known.

The demonstrated success of the passenger-focused RBS model demonstrates the value of its use in strengthening employee security. The WG believes that greater implementation of RBS is essential in continuing to shift the aviation security paradigm in a very positive and meaningful way. RBS has proven to be a significantly better system than what it replaced because it enables better allocation of resources and it focuses on identifying those with intentions to harm persons and/or property.

The WG applied risk management principles in considering aviation's tolerance, or exposure, to insider threats specific to airport employee screening/inspection, and has proposed appropriate mitigation strategies. The WG exercised an RBS approach that employed a process of identifying, evaluating and addressing these risks to mitigate the exposed vulnerabilities and to close any security gaps in airport access control. The risk-based system for employee screening and access control encompasses security screening and inspection, employee vetting, internal controls, intelligence and risk-based security, and security awareness.

On the Matter of 100 Percent Security Screening of Employees

Given the circumstances surrounding the alleged smuggling operation and calls by some members of Congress to conduct physical screening of all employees who are permitted access into secured airport areas, the WG believes that this subject deserves special attention. Accordingly, the WG has explored this matter at considerable length.

Although the WG determined that physical screening is one of several elements that should be used in combination to enhance access control, it is certainly not the sole means, nor should it be viewed as a standalone "solution."

For purposes of its discussion and this report, the WG defined 100 percent employee screening as the application of technical or other means intended to prevent the unauthorized carriage of prohibited and unauthorized items into secure and sterile areas. These processes would be applied to every employee each time they enter airport sterile and secure areas without exceptions/exemptions. This would include representatives of the military, armed government employees, law enforcement, emergency medical assistance personnel, and others.

A significant challenge in addressing this issue is that the WG could not find an example of 100 percent employee screening in the United States that would be equivalent to passenger screening. In several examples labeled "100 percent airport employee screening," the WG found that not all employee populations are screened to passenger standards. Numerous exceptions are allowed in screening eligibility, continuity and practices, and physical barriers to separate screened and un-screened employees did not exist. The WG also looked outside the U.S. for examples of "100 percent screening" and similarly found that due to nearly identical factors, none would qualify as 100 percent screening of 100 percent of all airport employees to passenger screening standards.

Certainly, physical screening is a fundamental security methodology and is a means, but not the only means or necessarily the best means, for deterring acts of criminality or terrorism within a defined space. The WG received reports that physical screening of employees has been implemented at some major airports on a voluntary basis; these measures were taken, in part, to address demonstrated levels of criminal activity involving carriage of illegal items/substances into airport sterile and secured areas.

However, security resources, whether measured in terms of infrastructure or personnel, provide a higher degree of risk mitigation when used in random and unpredictable ways, consistent with RBS. Static security measures, such as physical screening, can be studied, tested, and more easily circumvented than those that are dynamic and less predictable. No single measure can provide broad-spectrum protection against risks or adversaries. Therefore, risk-based, multi-layered security offers the greatest ability to mitigate risks through the application of flexible and unpredictable measures to protect commercial aviation.

Passenger screening is well recognized as a fundamental element of passenger scrutiny, but there are significant differences between the screening of passengers and employees. For example, employees are not necessarily screened/inspected at one fixed location. Employees are subject to screening/inspection in their work environment and must wear and/or carry with them metal objects, tools with sharp edges, and items

that are on the TSA prohibited items list in order to perform their jobs. Therefore, what is known about an individual employee—that is to say, the trust that is given to a person on the basis of their employment status and identifiable character traits—is of greater importance than the types of objects that he or she may carry into an airport's secured area. Law enforcement officers, as just one example of this principle, are authorized to carry lethal weapons into airport secured areas on the basis of their job requirements and demonstrated integrity.

The WG examined the infrastructure changes that would be necessary to deploy 100 percent screening at US airports. The WG concluded that neither the TSA nor the industry has the resources available at most airports to absorb the influx of all employees, nor are passenger screening checkpoints co-located with the most common work areas in the airport. As such, significant infrastructure modifications would be needed to facilitate 100 percent screening of employees, to include:

- Further reducing the number of access points through which employees enter the workplace;
- Building new screening facilities (FBOs, cargo facilities, parking areas, terminals, etc.);
- Staffing of employee checkpoints with dedicated and trained personnel;
- Purchasing or leasing screening equipment;
- Maintaining screening equipment;
- Reconfiguring airport terminals; and
- Installing infrastructure to separate screened from non-screened employees

The WG does not believe that 100 percent physical employee screening would adequately mitigate potential risks; physical screening is incapable of determining a person's motivations, attitudes, and capabilities to cause harm, among other limitations. Implementing such screening would divert resources from other critical security functions needed to mitigate other risks. In summary, the WG believes that the necessary infrastructure installations, workforce expansion, and airport reconfiguration to accommodate "100 percent screening" would be an ineffective outlay of significant security resources with limited security value.

During its deliberations, however, the WG did identify a number of measures that could increase the security of employee access controls without the limitations and significant expenditures associated with 100 percent physical screening as are described within this report.

AREAS OF ANALYSIS

The WG used an analytical model that followed the flow of typical airport employment and credentialing practices, i.e., pre-employment vetting, badging, arriving

at work and entering secure areas, performing daily activities, and leaving work. The WG categorized the model into five areas of analysis and generated recommendations in each:

- Security Screening and Inspection
- Vetting of Employees and Security Threat Assessment
- Internal Controls and Auditing of Airport-Issued Credentials
- RBS for Higher Risk Populations and Intelligence
- Security Awareness and Vigilance

Security Screening and Inspection

Prudence dictates an ongoing review and assessment of security procedures to determine their effectiveness in mitigating risk, coupled with operators making adjustments to further enhance security. In accordance with this risk-based methodology, random and unpredictable security measures provide the most effective means of enhancing employee security.

Although there is no perfect security system, the multiple layers—which can be routinely enhanced or modified—provide an effective means to secure passengers, employees, and facilities. A clear strength of this type of system is the unpredictable nature of the individual layers of security and the fact that many airport and aircraft operators exceed the baseline security requirements through the implementation of additional processes, procedures and technologies that consider and are adapted to their unique geographic locations and facility designs.

In accordance with current procedures, airport operators randomly conduct inspections of employees holding Security Identification Display Area (SIDA) badges at different locations on the airport. In addition, employees are subject to search, inspection or screening at any point, not just when they enter through an access control point.

Under TSA's Operation Playbook, TSA utilizes roving teams of Transportation Security Officers, Behavior Detection Officers, and Transportation Security Inspectors to conduct random and unpredictable physical screening/inspection of employees working in or accessing secured areas at direct access points. This security measure can be expanded as an effective tool for mitigating risk.

The combination of enhanced vetting, security awareness training, intelligence and information sharing, and random employee screening under Operation Playbook helps to mitigate the risk of prohibited items introduced at the perimeter. These items may go undetected using a fixed-point employee screening system. In addition to introducing a high level of unpredictability, and therefore deterrence, this type of random

and unpredictable screening/inspection program represents another formidable layer of security.

The WG believes that TSA should expand random employee screening/ inspection under Operation Playbook so that every employee entering or working in a secured area of an airport has the expectation that they will be subjected to screening/inspection. Airport and aircraft operators can support expanded Playbook operations by selectively closing access portals in order to route employees through the screening locations. Finally, airport and aircraft operators and law enforcement personnel should be invited to support Playbook activities, where practicable.

In setting the expectation that an employee is subject to being screened/inspected, the WG believes that establishing "randomness" in the context of employee access should include a science-based methodology. In developing such a methodology, game theory affords a framework to perform mathematical computations in security domains providing risk assessment and hazard prediction for enhanced decision-making. Game-theoretic analysis models the complex interactions between two or more agents (i.e., players) in conflicts of interest (i.e., games) in order to determine an optimal course of action (i.e., strategy) needed to reach a desired outcome. This type of solution provides the optimal, randomized strategy with measureable effectiveness while deploying limited resources to mitigate potential threats. This methodology is successfully used by military, law enforcement and aviation organizations.

RECOMMENDATIONS

1. DHS should immediately shift existing resources, as needed, to expand the TSA's random employee screening/inspection program (i.e., the Playbook to secured area access points.

2. TSA, in coordination and collaboration with government and industry subject matter experts and airport and aircraft operators, should develop an employee access security model using intelligence, scientific algorithms, and risk-based factors. This model should give all employees the expectation that they are subject to security screening/inspection at any time while working at an airport.

3. TSA should establish risk-informed, enhanced random screening/inspection for all employees, which would be increased on the basis of identified risk.

4. DHS should request from Congress needed funding for implementation of security measures for a to-be-developed employee access security model and the Playbook.

5. Airport and aircraft operators should prominently post signage at access portals or via other means to alert employees that they will be subject to screening/inspection in order to support compliance with random screening/inspection programs.

Vetting of Employees and Security Threat Assessment

Employee vetting involves a thorough review of a prospective or current employee's background to ensure that he or she has demonstrated the integrity to be given access to an airport's secure areas. This includes the Criminal History Records Check (CHRC), Security Threat Assessment (STA), and other database checks. Areas discussed during the WG deliberations ranged from enhanced connectivity among background databases for employee vetting to the challenges in vetting foreign national or foreign-born employees.

Background checks of employees who have been granted unescorted access privileges to the secured areas of airports have been required since 1985. Today, the regulated vetting process requires two critical parts: a CHRC and an STA.

Airport and aircraft operators are required by regulation to conduct an initial fingerprint-based CHRC on applicants seeking unescorted access to the SIDA. Fingerprints collected by airport and aircraft operators are forwarded to the FBI through TSA. The FBI and TSA return the applicant's Record of Arrests and Prosecutions (RAP) sheet, if any, to the airport or aircraft operator, and the airport or aircraft operator adjudicates crimes for which applicants were found to have been convicted within the preceding 10 years of a disqualifying criminal offense.

Each airport or aircraft operator must ensure that no individual is granted unescorted access authority unless the individual has undergone a CHRC that indicates that he or she has not been convicted of a disqualifying criminal offense in the prior 10 years. The initial CHRC is only required at the time of employment, which creates the potential for an employee to engage in criminal activity after their date of hire without the knowledge of their employer or TSA, and as a result, remain employed. The WG believes that real-time criminal activity monitoring should be part of the CHRC vetting process, similar to the perpetual vetting conducted by TSA for the STA.

In September 2014, as part of the implementation of its Next Generation Identification Program, the FBI introduced its Rap Back Service. The Rap Back Service provides authorized users the capability to receive immediate notification of criminal and, in limited cases, civil activity of enrolled individuals that occurs after the initial processing and retention of criminal or civil fingerprint transactions. The WG believes that TSA should accelerate the implementation of Rap Back with an immediate pilot with airport and aircraft operators and a goal of full implementation by the end of CY 2015. Implementation should ensure that airport and aircraft operators have direct and

immediate access to any activity or information reported through the Rap Back Service, as they do with the initial RAP sheet. The ability for airport or aircraft operators to review every applicant's criminal record and to make a determination about their ongoing suitability for unescorted access privileges is a critical layer of security.

TSA also should review the existing list of disqualifying criminal offenses to ensure it is comprehensive enough to address the current threat environment and to address changes within today's legal system. Many initial criminal charges are reduced to lesser offences based on plea deals or other criminal defense maneuvers that were not practiced on a large scale when the CHRC disqualifying criminal offenses were originally implemented. TSA should pursue, in consultation with industry stakeholders, any legislative or regulatory changes needed to update the list of disqualifying criminal offenses, to take into account how criminal charges and convictions are processed in the legal system today. This should include making a distinction between a charge and a conviction, identifying patterns of misdemeanors or other non-disqualifying criminal offenses, and expanding the limited look-back period and variances in look-backs from the date of application instead of the sentence-release date, and increasing the potential for permanent disqualifying criminal offenses. These disqualifying criminal offenses should also be referenced against other similar programs operated by DHS, U.S. Customs and Border Protection, United States Postal Service, and Department of Transportation.

The review of disqualifying criminal offenses should be done in the context of determining that an individual can be trusted to perform his or her job and responsibilities in a manner that poses no threat of intentional harm to themselves or others while in the secure areas of airports with access to aircraft. As a result, the WG also recommends that TSA review other eligibility criteria. For example, for the CBP-issued seal required for unescorted access to CBP-designated security areas at airports with international service, the employee must meet the qualifications for approval under the CHRC program and not have been convicted of any of 10 additional disqualifying criminal offenses. In addition, CBP may deny an individual a seal if the agency deems her or him a risk to the public health, interest or safety, national security, or aviation safety. Issuance of a seal also requires a certification by the employer that a "meaningful" background investigation has been conducted and that it has a need for this employee to access the CBP security area.

To build on this concept of eligibility criteria, the WG recommends that airport and aircraft operators introduce new certification language for badge applications that broadens the focus from existing regulatory requirements to a greater focus on overall suitability. Today, airport and aircraft operators must provide to the individual to be fingerprinted a fingerprint application that identifies the disqualifying criminal offenses and a signed statement from the individual that the applicant does not have a disqualifying criminal offense. Applicants must also sign a form authorizing the Social Security Administration to provide their social security number and full name to the TSA.

Example language of new certification language that broadens focus to personal accountability may read: “I acknowledge that I work in a position of trust and that if I misuse my badging privileges to circumvent any security system, measure, or procedure including smuggling of contraband or dangerous devices, I will be subject to civil and criminal sanctions, including the revocation of my badge and access privileges.”

TSA’s STA should be enhanced to include social security numbers, running all U.S. citizens against Systematic Alien Verification for Entitlements (SAVE), and fingerprints against DHS’ Automated Biometric Identification System (IDENT), and TSA Pre✓® Disqualifying Protocols. Identifying information of foreign nationals and foreign-born employees should be run against international databases. The addition of social security numbers and running all U.S. citizens against SAVE would help address the issue of identity fraud, which is an increasing concern. The use of biometrics to confirm identity at the time of badge issuance is another best practice aimed at combating identity fraud. Each element of this recommendation can be addressed separately, since each poses unique technical and regulatory/privacy challenges and timelines. The WG does not recommend precluding progress on certain elements while waiting for all elements to be added to the STA process.

Regarding watchlist vetting, TSA has indicated that it planned on eliminating watchlist access for U.S. airport and aircraft operators, and general aviation by mid-summer 2013. However, in coordination with the industry, a fully developed and implemented employee vetting process needed to be in place before watch list access was removed. Therefore, TSA agreed to partner with industry to discuss potential solutions for an automated approach.

Since satisfactory progress has not been made, the WG believes that a comprehensive review should be conducted by TSA to enable a web-based portal for industry use related to employee vetting. This process would ensure that the government is vetting all aviation employees and it would also allow the flexibility for aviation employers to vet a vast range of employees and new hire prospects not currently covered by regulatory requirements.

Regarding the vetting of foreign national or foreign-born employees, the WG believes that it is not presently possible to estimate the cost and effectiveness of a database or connectivity between existing databases for this purpose without additional details. Such an effort would entail regulatory or legal efforts to allow airports and airlines access to information beyond the current CHRC and STA processes. In the case of greater information on foreign nationals, it may require significant interaction with the FBI and foreign governments, Interpol and use of commercial vetting sources specializing in global vetting. This activity would have a potentially substantial cost that would have to be borne by the federal government.

RECOMMENDATIONS

6. TSA should accelerate the implementation of the FBI/Next Generation Identification (NGI) Rap Back Service with an immediate pilot with airport and aircraft operators with a goal of full implementation by the end of CY 2015. Real-time recurrency should be part of the CHRC vetting process, similar to the perpetual vetting conducted by TSA for the STA.

7. TSA should review the existing list of disqualifying criminal offenses to ensure that it is comprehensive enough to address the current threat environment and pursue any legislative or regulatory changes needed to update the list of disqualifying criminal offenses, other eligibility criteria, the addition of permanent disqualifying criminal offenses, extending the look-back period, and starting the period of adjudication on the individual's sentence release date or program completion date.

8. Airport and aircraft operators should introduce new certification language for badge applications that broadens the focus from existing regulatory requirements to a greater focus on overall suitability.

9. Airport and aircraft operators, in coordination with TSA, should review current training for Trusted Agents and Signatory Authorities and, as needed, provide enhanced training on identification documents, identity fraud, and behavioral analysis.

10. TSA should create and maintain a national database of employees who have had their airport- and/or aircraft operator-issued badges revoked for cause.

11. A comprehensive review should be conducted by the TSA to enable a web-based portal for industry utilization for employee vetting by TSA.

12. TSA's Security Threat Assessment should be enhanced to include SSN, running all U.S. citizens against SAVE, fingerprints against DHS' IDENT system, TSA Pre ✓® Disqualifying Protocols, and run foreign nationals and foreign-born employees against international databases.

Internal Controls and Auditing of Airport Issued Credentials

The WG has reviewed the effectiveness of the requirements for checks and balances currently in place to ensure the integrity, accountability, and control of airport-issued or recognized credentials over their life cycle. We have also broadly examined access privileges and procedures of various employee work groups to assess the effectiveness of internal controls.

Internal controls and audits are one component of an integrated risk management system designed to identify and mitigate threats associated with airport access control. These control measures work in conjunction with employee vetting, physical screening/inspection, intelligence, security awareness and training, and other risk-based security measures.

In the US and abroad, some airport-based employees have exploited their unescorted access privileges to secured areas to smuggle contraband, illegally place unscreened luggage on planes, and circumvent security screening for themselves, as well as unauthorized individuals. The prevalence of the insider threat—individuals who use authorized access to sensitive areas, equipment, or information to carry out or support terrorist or criminal actions—is increasingly concerning for the US aviation system.

Credentialing is an integral component of airport access control which governs both identification media and physical access to restricted areas. The credentialing process is regulated by the TSA. CBP regulates it for access to the Federal Inspection Service in international airports. Airport operators have controls in place to ensure accountability of airport-issued identification media, commonly referred to as badges, throughout the lifecycle of the badge. Regulatory requirements set the baseline for most, if not all, of these controls and airport operators across the country have implemented practices and solutions to meet, and in some cases, exceed these baseline requirements. Airport operators must also comply with regulations that prevent individuals who have not been granted unescorted access to secure areas of the airport from gaining unauthorized entry.

Existing regulatory requirements for airport identification systems are broad in scope and include the following requirements for airport operators:

- Outline a verifiable system in their Airport Security Programs to require airport badge holders, including air carriers, foreign air carriers, and tenants, to immediately notify the airport operator of any lost, stolen and/or terminated badges;
  - Retrieve and deactivate badges if they are lost, stolen, expired, or revoked
  - Terminate unescorted access authority or operational need
- Immediately remove or disable any access privileges associated with lost, stolen or revoked badges;
- Conduct comprehensive audits of all airport badges as well as audits of certain percentages of badges at prescribed intervals;
- Periodically renew and reissue all airport-issued badges, which includes collecting and deactivating existing badges;

- Reissue identification media to the entire badge holder population when lost, stolen or unaccountable badges exceed a set threshold, which is set at a very small percentage of the overall badged population;
- Immediately notify TSA if any part of the badging system or process has been compromised in any way;
- Secure unissued identification media stock and supplies.

The auditing program requirements for airport-issued identification media (i.e., security badges) are designed to ensure the integrity, accountability, and control of security media. Additional control measures that reduce the incidence of unaccountable and expired security badges, reclaim outstanding media, and verify operational need and authorized usage include audit, process, and policy enhancements. These best practices include proof-of-employment audits, work schedule audits, and field audits, which strengthen the airport's ability to mitigate threats and vulnerabilities associated with badging and access controls. Refer to Appendix 2 for a list of examples of audit and internal controls best practices for airport and aircraft operators to consider for implementation.

One of the significant challenges that airport operators face in maintaining accountability and control of airport-issued identification media and integrity of access control is the failure of authorized signatories to immediately report employee separations and lost, stolen, and unaccountable badges. This failure creates a security vulnerability that exposes airports and the entire air transportation system to potential criminal or terrorist activity. Additionally, airport operators and the TSA are exposed to reputational risk associated with deficient access control practices, as several of these incidents have been highlighted by national media outlets. The credential is the "key to the kingdom" and without adequate controls in place to mandate and enforce mandatory reporting of conditions which require immediate deactivation of access privileges, airport operators remain vulnerable and security systems are prone to compromise.

This type of lapse is a high security risk which deserves appropriate mitigation through regulating authorized signatories, as applicable. TSA should consider implementing a policy and penalties for non-compliance to enforce the requirement of Authorized Signatories to immediately report the following conditions to the airport's designated unit:

- Lost, stolen, unaccountable badges of their employees
- Employee separations

An extra enhancement to current credentialing is the use of biometric templates in the SIDA identification badge. This enables the confirmation of the identity of the card holder through mobile spot checks, or through biometric access control, and reduces the chances of a lost or stolen card being used by an unauthorized individual to gain access to secure areas.

Two mechanisms to effectively administer access control are to maintain the integrity of access privileges granted and minimize the number of physical access points located in restricted areas (i.e., Secured, SIDA, AOA, and Sterile Areas). Airport operators, in conjunction with tenant aircraft operators should identify opportunities to further restrict access privileges and/or further reduce access points as operationally necessary. This control measure encompasses changing the airport infrastructure to eliminate access portals which do not impact operations, and/or restricting access privileges through automation (e.g., reprogramming the security badge in the badging system, or by implementation of policy mandating operational need). A risk-based approach to implementing this measure would focus on the certain portals which include, but are not limited to, those which provide access from public areas to the restricted areas. Exemptions to this control will be necessary for certain employee work groups such as public safety and specified airport operations personnel, etc. It is recommended that tenants requesting access privileges to these sensitive areas require approval/authorization from the airline station manager and Airport Security Coordinator (ASC).

Enhanced CCTV monitoring and surveillance to observe employees at certain entry points and other areas, such as baggage make up rooms and cargo, is recommended to detect and deter insider and other illicit or unauthorized activity. CCTV monitoring, video analytics or predictive analytical software would focus on anomalies, behavioral patterns, carriage of bags, etc. This program could be modeled after the TSA Airport Surveillance Program (ASP) in which the airport enters into a co-share agreement with TSA and receives partial reimbursement of costs. TSA, in coordination with airport and aircraft operators, should enhance/expand the use of CCTV or other measures to monitor employees at certain entry points and other areas.

The recommendations presented in this integrated system of internal controls and audits are one aspect of an integrated risk management system designed to identify and mitigate threats associated with airport access control and employee screening/inspection.

RECOMMENDATIONS

13. TSA, and airport and aircraft operators should assess the efficacy of the auditing program requirements for airport-issued identification media (e.g., security badges) designed to ensure the integrity, accountability, and control of security media. Refer to Appendix 2 for a menu of options of audit and internal controls and best practices for consideration.

14. In cooperation with airport and aircraft operators, TSA should consider the establishment of biometric standards which may be used in identity verification

and badge validation. Included in this effort should be recommended standards and a cost/benefit analysis focused on implementing any such standards.

15. TSA should implement direct enforcement requirements upon authorized signatories associated with non-compliance, to include failure to immediately report lost, stolen, and unaccountable employee badges and employee separations.

16. Airport operators, in conjunction with tenant business partners, should identify opportunities to further restrict access privileges and/or further reduce access points as operationally necessary.

17. TSA, in coordination with airport and aircraft operators, should support the enhancement/expansion of CCTV or other measures to monitor employees at certain entry points and other areas, as necessary.

RBS for Higher Risk Populations and Intelligence

The WG evaluated the fundamental elements of RBS within the context of employee screening/inspection and identification of higher-risk populations. There is agreement that the items fundamental to this discussion include the identification of:

- Threats
- Terrorist methods
- Points of risk/corridors
- Methods of mitigation (screening/inspection protocols).

Identifying all of the above through the intelligence collection and analysis process is the key to preventing a terrorist event promulgated by self-radicalized lone wolves or returning foreign fighters.

RBS principles form the core of a successful security regimen, along with many commonly accepted procedures and industry best practices used in our Nation's air transportation system. A cornerstone of RBS is the continuous reevaluation of processes and protection measures in light of changing vulnerabilities, better understanding of risks, availability of new technologies, and the evolution of industry business practices.

It is because of these many different aspects of RBS and intelligence, that the WG reviewed the following areas: 1) intelligence-gathering methods and access to points of risk and risk corridors, 2) identifying and classifying personnel populations and assessing each population based on risk, 3) capturing, quantifying, and applying

intelligence input and airport risk, to drive screening/inspection methodology and rates, and other mitigation strategies based on the intelligence, threats and associated risks noted previously.

The WG recognized that as risk-based security measures continue to evolve, there is opportunity to apply them in emerging areas of concern, such as employee screening/inspection and airport access control. As noted above, central to RBS is the collection, analysis, communication, and application of intelligence information to develop and target evolving security mitigation measures, domestically and internationally. The WG determined that much of this overall intelligence mechanism is in place as relates to foreign countries, but elements of the mechanism are limited, or even severely limited, in certain areas of the U.S. The most notable opportunities for improvement include: collecting additional threat information through social media; improving the analysis of threat intelligence; expanding communication of domestically applicable intelligence information to the aviation community; and enhancing the application of classified and unclassified actionable intelligence information to benefit US airport RBS measures.

Critical to the aviation community's ability to effectively manage security risk is the identification of emerging threats. Current intelligence indicates that a primary method of communication between criminals, extremists, recruiters of radicalization candidates and pre-operational planners is through social media. Therefore, TSA should further explore the use of social media to track and assess emerging threats that may pose a threat to aviation.

When a threat stream is identified, monitoring of social media via keyword GEO Fencing at the appropriate airport, or monitoring of the social media of suspect employees, can be effective tools to determine the existence of an insider threat. The WG recognizes this approach can be contentious if not managed appropriately, but it is vital to today's security. It should also be noted that when a threat of this nature is identified, it is paramount that the information be shared with the appropriate airport and aircraft operators.

During the WG's review, concerns arose about several issues on this subject: the lack of aviation/operational subject matter expertise in the intelligence analysis process; the lack of a formalized sharing process at a meaningful classified level with those who have a real "need to know" to include airport and aircraft operators; and a breakdown in some areas of communication around emerging or imminent threats to airport and aircraft operators.

Based on these concerns, TSA needs to expand traditional domestic intelligence analysis methods and better convey domestic threats by airport location. One emerging option is the Air Domain Intelligence Integration and Analysis Center (ADIAC). This paradigm-changing initiative places industry subject matter experts alongside

government analysts in a classified environment allowing for a joint review of current intelligence streams and analysis of the threat posed to airport and aircraft operators. Additionally, a more formal process exists at the unclassified level for airport and aircraft operator personnel that requires the sharing of information about terrorist threat streams at specific airports. For strictly communication purposes, TSA could consider expanding appropriate platforms to provide greater information sharing between public and private sectors, especially as it relates to domestic threats. These measures are needed to support a focused surge screening/inspection operation.

With appropriate analysis of threat intelligence, TSA should expand/improve the existing City and Airport Threat Assessment (CATA) or similar program, to capture, quantify, communicate and apply applicable intelligence to inform airport mitigation measures. The advantage of well-analyzed intelligence is that it can be used to quantify levels of risk by airport that can then be used to determine risk-based security mitigation measures at each location. For example, the correlation and analysis of aviation risks can determine random and surge employee screening/inspection operations based on changing levels of risk, plus target higher-risk employee groups and specific points of risk/risk corridors within the airport perimeter.

Aligning threat analysis to security mitigation measures is a foundational element of RBS in that it provides the methodology to ensure the application of resources to the highest points of risk. To improve on the evolving risk from an insider-threat perspective, TSA should further analyze aviation insider-threat cases and create a model of predictive risk factors based on research and applied knowledge of the involved individuals and techniques used to circumvent security measures. This information can be utilized across the aviation community, as well as within the CATA program, and as an element of assessing risk associated with airport employee populations.

To accomplish this for employee screening/inspection and associated access control, TSA should develop a risk matrix for employee groups that are not presently eligible for RBS programs. As proposed, the matrix would quantify the risk associated with each employee group based on risk corridors and assign applicable risk-based security measures. Additional employee risk categories could be based on elements such as industry barriers to entry (e.g., requisite licensing to work in the industry), employee turnover rates, training requirements, access to more sensitive areas of the airport or highest valued targets.

The WG believes that there is a role for TSA, FBI and CBP to provide analysis that can be used to enhance employee training programs. Additionally, TSA should make it a priority to involve airport and aircraft operators in a discussion of the results of their security assessments to provide awareness of potential risks at each airport. As a result of this coordination, airport and aircraft operators will be better positioned to implement strategies to mitigate risks.

RECOMMENDATIONS

18. To foster the effectiveness of employee screening/inspection, TSA should consider the development of risk matrices for various employee groups using RBS principles.

19. TSA should maximize the dissemination of sensitive and classified intelligence collection as widely as practicable.

20. TSA should further explore the use of social media to track and assess emerging threats that may pose a risk to aviation. Analysis and best practices gained from this effort should be disseminated to regulated parties.

21. TSA should expand/improve the existing City and Airport Threat Assessment (CATA) or similar program to capture, quantify, and apply applicable intelligence information, and engage the aviation community in developing mitigation measures.

22. TSA should partner with airport and aircraft operators in conducting the Airport Risk Evaluation (A.R.E.) and provide the results of any and all risk and vulnerability assessments to appropriate regulated parties within the aviation community.

23. TSA should further analyze applicable insider-threat cases to create a model of predictive risk factors based on research and applied knowledge of the involved individuals and techniques used to circumvent security measures.

24. TSA, FBI and CBP should provide and make available enhanced training and information on insider threat activity and suspicious indicators that could be incorporated into airport and aircraft operator training programs.

Security Awareness and Vigilance

Promoting security awareness and vigilance throughout the aviation community is needed to help encourage employees take the initiative to identify and report suspicious activity. Effective security awareness necessitates that all members of the aviation community are cognizant of and embrace their responsibility for helping identify and mitigate potential risks.

In the context of employee access control, security awareness includes effective risk analysis, information sharing, employee training, and employee engagement. The WG encourages the TSA to make available to airport and aircraft operators the Federal Air Marshals' insider threat training and the Behavior Detection Officer behavioral analysis training. The WG believes that increased information sharing and coordination

when conducting risk assessments at airports will help ensure a cohesive approach to developing security countermeasures.

Initial and recurrent SIDA training programs can be further enhanced by incorporating specific information about security responsibilities, security awareness and reporting suspicious activity. Providing employees training that equips them with the skills to recognize indicators of suspicious activity and behavior will enhance their awareness and, through reporting programs, afford security officials increased awareness of potential areas of concern.

National reward programs can also provide an avenue for employees to report suspicious activity. These programs, such as the State Department's Rewards for Justice Program, have proven effective in providing the government and law enforcement agencies with valuable information. A similar program in the airport environment would enhance security by encouraging employees to report suspicious activity and behavior.

RECOMMENDATIONS

25. TSA should consistently provide briefings to airport and aircraft operators on the results of their security assessments to provide awareness of potential risks at the airport.
26. Airport and aircraft operators should be encouraged to develop and implement employee engagement/recognition programs aimed at promoting employee engagement in aviation security.
27. TSA, and airport and aircraft operators should promote existing national anti-terrorism reward/employee engagement programs to increase security awareness and reporting of suspicious activity.
28. TSA should promote or establish an existing or new Anonymous Tip Line to receive information from aviation employees who report a security concern or incident, and direct it to the appropriate regulated party(ies).

CONCLUSIONS

The WG was asked to study how vulnerabilities to airport sterile and secure areas are being addressed through existing TSA security programs, industry best practices, methods of employee screening/inspection used inside and outside the US, make airport visits, and report to the TSA within 90 days. The ASAC's recommendations were developed within the context of RBS, a holistic approach to aviation security. This approach acknowledges the globally interconnected aspects of the US air transportation system, the varied infrastructures supporting it, the availability

of robust employee pre-screening systems, and the need to apply aviation security resources efficiently and effectively.

The WG's recommendations focus on activities under the jurisdiction of the TSA granted to it under the Aviation and Transportation Security Act (ATSA, Public Law 107–71 November 19, 2001). We fully expect that these recommendations, when implemented, will concurrently mitigate the threat of terrorism and criminal activity in the sterile and secure areas of airports.

The WG began its work by investigating the practicality of performing 100 percent physical screening of employees, as called for by some individuals in the wake of the afore-mentioned gun smuggling revelations. The WG concluded that such employee checkpoints would not be a "silver bullet" and that there were other more effective and less costly methods of securing the sterile areas of airports. The WG does not believe that the inclusion of so-called "100 percent screening" as a layer of airport security appreciably increases the overall level of system-wide protection, nor would it lower overall risk.

The WG's twenty-eight (28) recommendations address items requiring varying degrees of Congressional and Department of Homeland Security support and a preliminary cost categorization. The WG calls for accelerated resourcing for these items. The WG has also identified areas where additional study may be warranted. The recommendations are, to a large extent, interdependent and do not stand alone.

The WG strongly urges TSA to inform its future actions in regard to employee screening/inspection and access control by the group's 28 risk-based and community-driven recommendations. Any actions taken by TSA, absent specific, credible threat information, should be made through the notice and comment process which affords stakeholders the opportunity to provide input.

The ASAC would like to thank TSA Acting Administrator Carraway and his staff for fully supporting the work of this group. We would also like to acknowledge the role of the Homeland Security Studies and Analysis Institute for providing data and expertise that strengthened many of our recommendations.

Appendix 1

Briefings from Aviation Security Experts and Reports

The WG received briefings from the following aviation security experts:

February 2
- Summary of 2008 airport employee screening pilot program, Rick Kohout (Homeland Security Studies and Analysis Institute (HSSAI)
- Insider threats, Tom Francis (TSA/OIA)
- Threats and vetting, Julie Carrigan (TSA/OIA)
- TSA security program and related compliance activities, Fred Stein (TSA/OSO/Compliance)
- International security issues, Craig Lynes (TSA/OGS)

February 11
- Summary of employee screening activities at the Miami International Airport, Paul Wisniewski (TSA/OSPIE)
- European Union/United Kingdom airport employee screening methods, Gareth Alston (United Kingdom Embassy)
- TSA vetting procedures, Steve Parsons (TSA/OIA)

March 3-4
- Hartsfield-Jackson Atlanta International Airport (ATL) security perspectives, Miguel Southwell (ATL General Manager)
- TSA Pre✓®application process, Don Lombardo (TSA/OIA)
- TSA Behavior Detection Officer (BDO) program, Mike Silata and Kim Levesque (TSA/OSO)
- TSA Pre✓® implementation and managed inclusion, Bryan Quaid (TSA/OSO)

During its deliberations, the WG reviewed the following reports:
- *TSA's Security Screening Procedures for Employees at Orlando International Airport and the Feasibility of 100 Percent Employee Screening* (OIG-09-05), October 2008 (Sensitive Security Information (SSI)), Department of Homeland Security (DHS) Office of Inspector General (OIG)
- *TSA Airport Employee Screening Pilot Program: Final Report*, HSSAI, December 2008
- *Aviation Security: A National Strategy and Other Actions Would Strengthen TSA's Efforts to Secure Commercial Airport Perimeters and Access Controls* (GAO 09-399), September 2009, GAO
- *TSA's Oversight of the Airport Badging Process Needs Improvement* (OIG-11-95), July 2011 (SSI and non-SSI versions), DHS OIG

Appendix 2

Audit and Internal Controls Best Practices

1. Proof-of-Employment Audit
   Require proof of active employment for each badge holder which may include, but is not limited to, a company time and attendance record, human resources (HR) or payroll record, or letter from HR or company headquarters confirming employment. This audit is one of the most effective internal controls to identify badge discrepancies resulting from a failure of the authorized signatory to notify the airport to deactivate the badge of a separated employee.

2. Change in Employment Status Policy
   Implement a change-in-employment-status policy which governs the custody and status of security badges of individuals whose employment status has changed in accordance with the following conditions: Family and Medical Leave Act (FMLA), worker's compensation, military service, reassignment, or other extended personal time off, etc., which no longer supports the operational need to maintain possession of a badge. Authorized signatories are required to temporarily deactivate and maintain secure custody and control of the media. Long-term absences will require the media to be permanently deactivated. This policy reduces the number of lost and unaccountable badges during extended absences from work.

3. Field Badge Audit
   Conduct a random field badge audit at the Authorized Signatory's place of business. During the site inspection, the auditor conducts a document review and interview of the Authorized Signatory to assess compliance with badging requirements and information protection (i.e., Sensitive Security Information and personally identifiable information), and best practices.

4. Work Schedule Audit
   Reconcile the badge holder's work schedule with Access Control System (ACS) transactions during a specified period to identify access anomalies or irregularities, such as an employee using his/her badge at the airport outside of work hours. This audit may be conducted using manual or automated reconciliation of ACS and work schedule records. The company's Authorized Signatory provides the work schedule of randomly selected employees to airport security representatives for comparison with the employee's badge activity utilizing ACS records. Insider threat software procured by an airport operator offers this automated capability; however, a data feed from the employer, e.g., aircraft operator is required.

5. Deactivated Badge Use Audit
   Conduct a deactivated badge audit to identify unauthorized use of a deactivated

badge (e.g., access was attempted but not granted) by performing a forensic review of ACS transactions.

6. Reverse Badge Audit
   Conduct a reverse badge audit which requires the company's authorized signatory to provide an internal report of their badge holders that is reconciled with the control record of the security badge office to identify discrepancies.

7. Badge Deactivation for Non-Use
   Consider deactivation of badges which have been inactive for a defined period of time. This measure will assist in reducing the lapse time of badges not immediately reported as missing or that are no longer needed. If an employee's badge is deactivated as a result of inactivity, the company is required to provide the Security Badge Office with a legitimate reason for the inactivity (e.g., FMLA, military leave, etc.) upon which the badge may be reactivated. During extended absences, the employee may need to submit a new badge application. Exemptions based on specific employee assignments and positions will be necessary.

8. Biometric Confirmation of Identity for Badge Issuance and Random Auditing
   Capture a biometric template of SIDA applicants (e.g., fingerprints or other biometric) at the time of submitting fingerprints for CHRC processing. Confirm identity of applicant at the time of badging by matching the individual's biometrics to the template originally captured. Retain the biometric template of each individual on their SIDA card for random checks with mobile biometric readers in the secured area to confirm the identity of the card holder and ensure that a card is not being used by someone other than the person authorized for SIDA privileges.

Appendix 3
Members of the Airport Access Control Working Group

Steve Alterman
President
Cargo Airline Association

Paul Arnold
Director, Aviation Security
United Parcel Service

Christopher Bidwell
Vice President, Security and Facilitation
Airports Council International – North America

Alan Black
Vice-President of Public Safety
Dallas Fort Worth International Airport

Scott Broyles
President and CEO
National Safe Skies Alliance

Colleen Chamberlain
Vice President, Transportation Security Policy
American Association of Airport Executives

Liam Connolly
Senior Director- Regulatory Affairs
Regional Airline Association

Sean Cusson
Director Public Safety and Security
Airports Council International – North America

Denny Dillard
President
Dillard Group International

Ken Dunlap
Director, APCS Government Affairs
International Air Transport Association

Robert Francis
Senior Policy Advisor
Zuckert Scoutt Rasenberger

Michele Freadman
Deputy Director, Aviation Security Operations
Massachusetts Port Authority

Randy Harrison
Managing Director, Corporate Security
Delta Air Lines

Jens Hennig
Vice President, Operations
General Aviation Manufacturers Association

Stephen Holl
Chief of Police
Metropolitan Washington Airports Authority Police Department
Airport Law Enforcement Agencies Network

Cedric Johnson
Director, Office of Airport Security
BWI Thurgood Marshall Airport

Janulyn Lennon
Director of Security
Hartsfield-Jackson Atlanta International Airport

John McGraw
Director, Regulatory Affairs
National Air Transportation Association

Jeanne Olivier, A.A.E
Assistant Director, Aviation Security
Port Authority of New York and New Jersey

Eric Thacker
Managing Director, Security
Airlines for America

Diana Vezzetti
Aviation Security Specialist
Air Line Pilots Association, Int'l

Gary Wade
Vice President Security
Atlas Airlines

Chris Witkowski
Director Air Safety, Health and Security
Association of Flight Attendants

Jerry Wright
Manager, Aviation Safety & Security
Air Line Pilots Association, Int'l

Richard Kohout
Mission Area Director, Counter-terrorism, Borders, and Immigration
Homeland Security Studies and Analysis Institute

Adrian Smith
Senior Analyst
Homeland Security Studies and Analysis Institute

Dan McCann
Transportation Security Administration

Shaina Pereira
Transportation Security Administration

Don Thompson
Cross-Modal Division Director; Executive Sponsor of ASAC Working Group on Airport Access Controls
Transportation Security Administration

Dean Walter
Transportation Security Administration

Paul Wisniewski
Transportation Security Administration