SAFE SKIES

PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0006

February 2017

Employee Inspections Synthesis Report

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Harold Flamenbaum
Dave Fleet
Ross Gaisor
Zach Varwig
Faith Group, LLC
St. Louis, MO

COPYRIGHT INFORMATION

NOTICE

The project that is the subject of this report was a part of the Program for Applied Research in Airport Security (PARAS), managed by Safe Skies and funded by the FAA.

The members of the technical panel selected to monitor this project and to review this report were chosen for their special competencies and with regard for appropriate balance. The report was reviewed by the technical panel and accepted for publication according to procedures established and overseen by Safe Skies.

The opinions and conclusions expressed or implied in this report are those of the individuals or organizations who performed the research and are not necessarily those of Safe Skies or the FAA.

Safe Skies and the FAA do not endorse products or manufacturers.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the Airport Security Systems Integrated Support Testing (ASSIST) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the Program for Applied Research in Airport Security (PARAS), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request for proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies Special Programs Manager*

PARAS 0006 PROJECT PANEL

Alan Black *Dallas/Fort Worth International Airport*
Chris Bidwell *Airports Council International – North America*
Colleen Chamberlain *American Association of Airport Executives*
Eric Thacker *Airlines for America*
Ken Harwood *Greater Orlando Aviation Authority*
Randy Harrison *Delta Air Lines*

CONTENTS

SUMMARY

Employee inspections hold many challenges for airports. The task for airport administrators is to create an environment where employees have a reasonable expectation that they and their property may be inspected at any time. Airports have approached the subject of inspections and insider threat in different ways in order to be as effective and efficient as possible with very limited resources. At the time of this report, airports, while faced with many physical and logistical challenges, have developed best practices in order to accomplish the goals of the TSA-released Security Directives and Information Circulars that were based in part on the 28 recommendations by the Aviation Security Advisory Committee working group. Examples of these best practices include internal controls, badge audits, methods of handling higher risk employee populations, and security awareness/outreach programs to add layers of vigilance. Managing such processes and procedures, even after thoughtful development, has proven to be difficult.

The airports' individual challenges have caused them to look for ways to share the responsibilities of employee inspections. Teaming and coordinating with the TSA and the use of security contractors has proven to be an effective approach. It must be noted that at the outset of this project, airports reported that air carriers were not performing inspections. More recent responses and follow-up communication with airports now indicate that air carriers have, in fact, begun to perform inspections and employee screenings.

Overall, responding airports have put together various forms of inspection teams that use a random approach. Most inspections are executed stadium style. Many airports perform additional random inspections of employees in the Secured Area and include Challenge or Compliance Teams. Challenge Teams are formed by airport security (or an authorized airport security representative), and use two methods when in Secured/SIDA areas: (a) hide their badge, approach employees, and see if those employees will challenge them to display their ID badges (some airports reward the challenging employee with a gift card or cash), or (b) approach employees at random and ask to see their badges (in some cases, portable card readers are used to validate the badge and accessible items are inspected).

In addition, a few airports have acquired screening equipment in order to provide a standalone employee checkpoint. In a further attempt to be as innovative, efficient, and effective as possible in managing employee inspections and the insider threat, some airports have implemented or plan to implement new identity management and access control analytic software programs. These programs use artificial intelligence or rule-based analytics to identify unusual employee access and egress in terms of locations, time, and frequency.

It must be noted that none of the airports or airlines who were interviewed, responded to surveys, or provided information for this synthesis effort conduct 100% employee inspections. Essentially, all indicated that conducting continuous, random, and unpredictable inspections and performing additional vetting and audits were effective deterrents and more economically feasible.

PARAS ACRONYMS & ABBREVIATIONS

The following acronyms and abbreviations are used without definitions in PARAS publications:

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
ANSI	American National Standards Institute
AOA	Air Operations Area
ARFF	Aircraft Rescue and Firefighting
CCTV	Closed Circuit Television
CDC	Centers for Disease Control and Prevention
CD/DVD	Compact Disc/Digital Video Disc
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
EPA	Environmental Protection Agency
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
ID	Identification
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
KPI	Key Performance Indicator
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
R&D	Research and Development
ROI	Return on Investment
SIDA	Security Identification Display Area

SOP	Standard Operating Procedure
SSI	Sensitive Security Information
SSN	Social Security Number
TCP/IP	Transmission Control Protocol/Internet Protocol
TSA	Transportation Security Administration
XML	Extensible Markup Language

INTRODUCTION

A real and growing concern among airports and airlines is the possibility of an insider threat; someone who has been granted unescorted access authority to the Sterile and Secured Areas can use that access in the commission or facilitation of a crime or act of terrorism. Through the Risk-Based Security concept, airports and government agencies have developed various methods of detecting and preventing these nefarious activities. Employee inspection is one of these methods.

Current regulatory requirements have airport operators randomly inspecting airport workers, employees, and other individuals entering Sterile and Secured Areas of the airport. In response to recent events, individual inspection has become an area of intense focus for airports and government agencies. In their Final Report released in April 2015, the Aviation Security Advisory Committee Working Group suggests that "…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." Accordingly, many airports are actively enhancing or attempting to enhance their inspection practices.

Section 1 of this report focuses on the synthesis team's interaction with the airports and airlines via surveys, emails, and follow-on interviews.

Section 2 provides the best practices that were either volunteered by airports and airlines or were derived from the team's follow-on interaction. Best practices are arranged by airport category, and have been de-identified in order to protect specific airport/airline information. Practices and procedures are presented in general terms.

Appendix A contains the survey questions, and Appendix B provides a discussion on the data gathering.

OBJECTIVE

The objective of this synthesis is to create a useful resource for airports and airlines to review the methods and best practices that airports of all types and sizes within the United States are currently or considering using to inspect individuals and manage the insider threat. This report summarizes the existing guidance and effective practices that were gathered through surveys and interviews with airport operators and airlines.

SECTION 1: Survey and Interview Results

A summary of the survey and interview results is provided in this section in narrative form for ease of understanding. The complete survey is contained in Appendix A for reference.

The Research Team feels sufficient information was collected to draw reasonable conclusions and present a fair representation of the industry. A narrative description of the data and information gathering process is contained in Appendix B.

1.1 General Findings

The following findings represent an overall look at the industry's current state of employee inspections. The information is generalized, yet is specific enough for airport and airline staff to use this report to improve existing operations and update and/or develop workable employee inspection processes.

As with any airport or airport-related function, the team found that most airports accomplished similar tasks but chose implementation approaches that best reflected the airport's physical configuration and operation. Airlines indicated that their programs and efforts were in coordination and cooperation with the airports where programs were implemented or planned for implementation.

The team did note that in almost all cases, regardless of airport size, concerns were raised about implementing any new program in the middle of a budget cycle, given the known and anticipated costs associated with employee inspections.

1.1.1 Employee Inspections – Overall

Airports have reported that they have closed as many access portals as possible. The remaining minimum number of portals were needed in order to support their day-to-day operations. Airports indicated that they are performing various forms of random employee inspections at these access points. A majority of airports reported that they are continuing to work hard on their inspection programs, which they feel are well considered and well planned. Airports also believe that they have worked closely with their local TSA offices to ensure success of their programs.

Where budgets have allowed, airports indicated that they typically utilize a contracted guard force to perform randomized inspections. The term "random" as defined by different airports and airlines resulted in various forms of inspection program implementations—from random selection of access portals to random employees and bags being selected for inspection, or various combinations of both. Some programs require 100% presentation of employees at the inspection location, where employees (and their property) are randomly selected for inspections/screening. All programs, however, had the intent of adding a level of unpredictability such that the employee expected that they (or their belongings) may be selected for inspection (or some form of screening).

Whether inspections are conducted by airport staff, Law Enforcement Officers (LEO) or contracted guard forces, with the exception of airports that have installed screening equipment, airports and airlines report that they are conducting stadium-style inspections of airport workers. This typically consists of visual inspection of accessible property, to include having employees open bags, backpacks, briefcases and packages.

Surveyed airports reported that all inspections included identification checks, often with portable readers. Some programs implemented or planned the use of screening equipment such as x-ray and explosive trace detection (ETD) machines. One inspection program included the random use of ETD equipment to screen employee bags even if the employee was not selected for inspection, or screen the employee but not the bag. One airport indicated that they also look at tracking/identifying where the employee is supposed to be at that particular time of day. This practice requires integration of specialized technology software with the airport's access control system (ACS).

Most airports reported that they coordinate their inspections with TSA's Playbook efforts. This is a risk management approach to creating unpredictability in the security measures it uses, with the agency detailing 120 "plays" for officials to use randomly. One airport indicated that inspections are done by TSA during Playbook activities. A few airports indicated that, due to outside limiting factors and budget constraints, random inspections are performed by airport staff. However, some airports indicated that they often do not participate with TSA so that more inspections can take place resulting in better utilization of limited resources.

Where airlines are involved with inspection programs, they indicate that they work in close coordination with airports and local LEOs.

Many airports reported reviewing historical ACS data to aid in making determinations for locations and times of inspections.

Airports report that while most Sterile Area employees must use the TSA checkpoint to gain access to the Sterile Area, not all checkpoints have been configured with ACS badge readers to validate active badges. Some airports are in the process of installing ACS badge validation readers at all Travel Document Check (TDC) locations. A very limited number of Sterile Area workers were provided with SIDA badges in order to support the operation. These airports report that badge holders often have limited access via specific doors and those employees are subject to inspections.

A few airports indicated that they have tried to implement innovative programs; for example, they set up inspection locations inside stairwells that are typically used as workforce commuting stairs.

Most airports, when asked if they plan on implementing formal designated locations for employee inspections, indicated that they do not and would not unless mandated and/or funded by TSA.

Some airports are planning or have implemented the use of ACS and ID management analytics software to review historical access control data to support their inspections process as well as to look for access behavior anomalies as part of their insider threat mitigation strategies. Additionally, some airports and airlines indicated that a holistic approach to employee inspections includes continuous employee vetting, using programs like Rap Back[1].

Airports have also reported that airlines have either implemented or are planning to implement employee screening for their own employees. This could possibly influence other airlines at the same airport to implement similar programs for their employees.

1.1.1.1 Employee Inspections – Management

Airports and airlines develop and manage their inspection programs and oversee the contract guard force that carries out the actual inspections. The airports and airlines typically audit the guard force on a

[1] The FBI Rap Back service allows authorized agencies to receive ongoing status notifications of any criminal history reported to the FBI after the initial processing and retention of criminal or civil transactions.

random basis. Where inspections are being carried out by LEOs on behalf of the airport, the Airport Security Coordinator typically reviews these requirements with the LEO.

Some airports reported performing a good deal of ACS data mining, which they felt was necessary in order to establish optimum schedules. They are also providing this level of coordination with TSA, and when available, supplying the TSA with a portable/mobile verification reader for use when performing inspections. While it may not be a trend, a few airports reported that they are currently implementing or plan to implement software with analytic tools to find access anomalies or potential suspicious behavior.

Airports also reported that, while they can perform inspections of accessible property, they were concerned about their inability to legally go beyond inspections and perform searches and/or full screening due to local, county, state, or other governing body ordinances.

One airline has programmed and implemented a randomizer running on an iPad, which is used to select employees and their bags for inspection.

Most airports have implemented signage indicating that employees are subject to search. An airport reported that they have implemented stickers at doors indicating who (what groups) may perform searches. Many airports reported that their badge applications indicate that Aviation Workers (AW) are subject to airport rules and regulations; in some cases the application states that AWs understand that they are subject to search.

Employees not wishing to be subjected to inspections are typically presented with a rules violation. Many airports reported implementation of a progressive fine structure including suspension. One airport indicated that for inspection violations, their program includes loss of SIDA/sterile door access privileges such that non-compliant AWs must use the Security Screening Checkpoint (SSCP) in order to gain access to their work location.

1.1.1.2 Employee Inspections – Limiting of Bag Size

Much discussion has taken place relative to limiting the size of a bag that an employee can bring into the secure area, limiting the number of bags, or even requiring that the employee carry a clear bag or backpack.

While some airports reported that they would like to implement a clear bag policy, they have not yet done so. Others indicated that although the airport had not, tenants at their airport have begun giving out clear bags for employees. Some airports indicated that tenants and airlines at their airport have requested that AWs limit the number of bags and bag sizes that they carry; a few airports have specifically limited the bag size. Most airports, however, have reported observing that as employee inspections have increased, AWs started reducing the number and size of the bags they carry on their own.

One airline indicated that their programs included the furnishing of clear backpacks to aid in the search process.

Additionally, some airports reported observing that contractors tend to no longer bring all their tools in and out, but rather, leave their inspected tools in offices and work places to make it easier for them to get into work areas in a timely manner.

1.1.2 Gate Inspections

Most airports indicated that they have some level of security staff, usually contract security, at secure area access gates where inspections take place. Many airports indicated that they do not have any unmanned inbound gates that provide access to the Secured Area. Others are looking to close and/or eliminate unmanned and/or non-ACS controlled perimeter gates.

Airports reported a variety of gate-related inspection processes; some airports perform a full visual check of each vehicle, including an undercarriage inspection to look for anomalies, while the inside of the vehicle is not inspected. Some airports perform continuous, random inspections where all doors/trunk/rear of the vehicle are opened and items are inspected. Others indicated that they were challenged by finding a balance between the flow rate and the thoroughness of their vehicle inspections program. One airport indicated that with a large perimeter and many gates, the purpose of their inspections program was to look for large IEDs.

A number of airports indicated that they perform employee inspections at gates that include visitor/escort processing. While some airports log the visitors being escorted, others have implemented a system to vet visitors through an internal process that includes a combination of internal violation notices as well as the no-fly and selectee listings.

Airports indicated that they also perform random ramp inspections, including creating choke points for all traffic leaving their terminal area where they perform inspections of all vehicles and personnel. Another airport indicated that they initiate rolling traffic stops where they perform inspections, including the use of a mobile ACS badge validation reader.

1.2 Insider Threat, Risk Based Security, Audits, and Security Awareness Programs

Airports and airlines indicated that, as part of their employee inspections program, they have implemented or plan to implement some level of insider threat mitigation, additional audits, risk based security efforts, and additional security outreach and awareness programs. Listed in Section 1.5 Best Practices are examples of some creative programs.

1.2.1 Insider Threat and Risk Based Programs

Some responding airports have implemented insider threat teams or programs. Airports reported the use and/or planned use of technology, such as ID management systems with analytics, to review ACS history and look for access anomalies. In many cases, the insider threat team utilizes information from analytics, the inspection program, CCTV surveillance, and tip reporting hotlines. They then use the tips received to start or further investigate issues, thereby adding additional layers of intelligence in support of their overall employee inspections programs.

While multiple airports reported the implementation of undercover detectives to support their inspections and insider threat programs, a few airports have added auditors and/or staff to support data analysis. One airport indicated that they have implemented software tools to support the optimization of not only their employee inspections program, but also their random vehicle inspections. Still, one more airport indicated that they have hired a full-time intelligence analyst to support the inspections program by reviewing ACS, ID, and audit data.

Airports reported implementing innovative methods such as assigning one unique ID to each person, so that any violations related to that employee follow him or her. Under these types of programs, all data about the employee, including all issues and notices of violations, are not based on that employee's current badge or a badge associated with any particular employer. The airports indicated that this is essential, especially with high risk, high turnover populations, noting that many lower wage employees work multiple jobs at the airport, and often leave and come back. Additionally, one airport indicated that they have created their own internal watch list, which combines airport violations with the TSA's no-fly and selectee listings to allow them to better vet their population, including those AWs who are no longer working at the airport but who potentially return for a specific project needing an escort.

Airlines reported that they are reviewing their hiring and vetting practices. This includes going beyond the base required disqualifying crimes, the potential use of third-party firms to review employees, and suspicious behavior reporting programs and mechanisms. They want their employees to become accustomed to being inspected/screened. At the same time, airlines want to be respectful of their employees' time, so they are using concepts that require 100% presentation for inspection while performing continuous, random inspections.

1.2.2 Company and Employee Badge Audits

Airports have taken some innovative approaches to badge and employee audits to support the employee inspection process. While all airports report a working and effective authorized signatory training program, multiple airports have begun requesting that authorized signatories provide the airport with their list of who they believe are active badge holders. One airport indicated that they have begun inserting bogus names to company badge audits. In addition to standard quarterly audits, airports have begun to perform targeted audits.

Additionally, many airports reported that all new employees get a 6-month badge, which can then be extended to 1 year and up to a maximum of 2 years. One airport indicated that they start with a 3-month badge for high turnover groups. While this practice puts additional administrative strain on the airport, it allows tighter controls on their most suspect population where there is the potential for the highest level of turnover.

SECTION 2: Best Practices

Information provided in this section covers employee inspections and inspection-related best practices conveyed to the team during follow up discussions. We have categorized and combined these best practices in the following logical groupings:

- **Technology –** Implementing new technologies, or repurposing technology, such as analytics to evaluate unusual behaviors of staff and badged personnel
- **Policies and Procedures –** Managing access control programs, setting inspection protocols, rules and regulation violation assessment and adjudication policies and processes.
- **Facilities –** Adding or modifying physical security areas and assets
- **People –** Utilizing various resources to aid in intelligence gathering
- **Other –** A catch-all category of good ideas

In addition to placing best practices in categories, we have identified what we feel are the pros and cons of each best practice and their applicability to airports of different sizes. The advantages and disadvantages identified in the report are based on the expert opinions of the authors of this report.

2.1 Technology

2.1.1 Portable/Mobile Validation Card Reader

- Badge readers can be deployed to validate the status of cardholders randomly during inspections in the Secured/SIDA, including random Ramp locations.
- Readers can be deployed to non-ACS gate locations as needed to validate employee badges.

Pros: Part of the TSA playbook recommends unplanned and random inspection of credentialed workers with approved ACS badge readers. This is a good audit tool, knowing badged personnel will and can be screened anywhere on the SIDA.

Cons: It takes time to set up the temporary screening area and resources, in addition to the investment of portable/mobile ACS badge readers.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	May be cost prohibitive

2.1.2 Fixed Badge Readers Deployed to SSCP Lanes Designated for Employee Screening

- Badge readers can be deployed at TDC locations/lanes designated for employee screening to validate active status of employee’s badge.

Pros: This closes the door to potential misuse by employees with deactivated IDs being able to get into the Sterile Area. This is a good audit and control tool. Expired and deactivated badges can be taken from the employee.

Cons: The option requires additional costs for the procurement and installation of the SSCP Validation Card readers.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

2.1.3 Biometric and CCTV Enhancements

- Airports report implementation of multiple layers of ACS authentication readers and innovative CCTV surveillance programs they use in conjunction with their overall employee inspection program.

❖ Example: Use of multiple levels of access control to gain access to the facility where biometric access readers (or other multifactor authentication devices) are installed at facility entrances and/or unscreened public-to-Secured/Sterile portals to validate employees. These doors are all equipped with CCTV. While biometric access readers are utilized at the facility entrance, an access control card plus pin reader may only be required to gain access to the next security boundary level or area. Access to spaces within the same security boundary level may just require the use of a card reader.

Pros: Adding a layer of security with visual and biometric authentication is extremely valuable and offers 100% employee validation for specific locations, such as unscreened public-to-Secured/Sterile access portals. These solutions provide personal authentication and offer a real deterrent to unauthorized access. They can also be deployed at perimeter gates and other critical control points. Implementation enables quick, secure, and authenticated access while reducing personnel costs. This option is highly suitable for large airports.

Cons: There is a significant capital improvement investment in deploying these solutions. Costs are variable depending on the number of access points; however, there is a high initial fixed investment in infrastructure and equipment. Both capital improvement dollars for system acquisition and integration into the ACS, as well as operational dollars for maintenance and support must be planned. Investment in this technology requires a relatively high cost of entry and may be cost prohibitive for smaller airport operations that have too many public-to-Secured/Sterile access points to justify the expense.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	May be cost prohibitive

2.1.4 Randomizer Tablet

- Use a portal device such as a tablet with a randomization program to select employees and/or their goods/bags for inspections.

Pros: The use of a randomizer is a fair and equitable method for making inspection selections in conjunction with the airport’s overall employee inspection program. It can aid in the employees’ acceptance of the program since it ensures that selections are truly random. In this way, 100% of employees present themselves for inspection, and the randomizer makes the selection and tracks the number of individuals being inspected. This is highly suitable for all airports.

Cons: There is a capital improvement investment in deploying the solution and training the inspection force.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

2.1.5 Identity Management Systems with Data Analytic Capabilities

- Identity and credential management implementations aid in managing the airport’s complex environment.
- Provides automated enrollment, watch list comparisons, fingerprinting, background investigations, employee training, and access privileges
- Supports data mining and aids in discovering access control anomalies
- Supports complex audits
- Provides for more accurate reporting and analysis

Pros: An identity or credential management system supports the airport’s security program by automating badging and access control tasks, and can be used to proactively audit, report, and analyze access control activity. Integrated identity management systems can increase/modify security levels at selected access points as needed; these systems also allow for role-based access control for areas that are approved for the employee’s access.

Cons: These systems can be costly from a procurement, implementation, and airport staffing and support standpoint, and may be cost prohibitive for smaller airports.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	May be cost prohibitive	May be cost prohibitive

2.1.6 Unique ID for Each Employee

- Issue a unique identification number for each employee, so that no matter how many times that employee comes and goes at the airport, and no matter how many employers/sponsors hire that person, violations or issues associated with that employee are recorded in the credential database.

Pros: This method ensures that the airport can track any employee’s rules violations or other issues that relate to the employee’s ability to maintain unescorted access at the airport.

Cons: This requires an identity or credential management system capable of supporting this best practice.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	May be cost prohibitive

2.2 Policies and Procedures

2.2.1 Disable Badges for Contractor Employees Who Are Not Always on Site

- The airport disables badges for contractor employees who are not stationed at the airport or who are not routinely at the airport. Contractors must get approval before coming to the airport in order for their badges to be activated.

Pros: This practice ensures that only contractors with specific on-site requirements are within the Secured/Sterile/AOA regions of the airport at specific predetermined times of day.

Cons: This method adds work to the badging office and supporting departments that must preplan and prearrange non-site-based contractor visits.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

2.2.2 Additional Sponsor Interview Prior to Badging

- Interviewing sponsors on why a new person needs a badge
- Helps the airport determine the minimum access needed for the new employee

Pros: This practice ensures that the sponsor understands and can explain what the new employee will be doing and where the employee will be working; it also helps communicate the need to control airport access.

Cons: This method adds work to the badging office.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

2.3 Facilities

2.3.1 Centralized Goods and Delivery and Inspection Location

- All goods for the airport arrive and are inspected, marked, and sealed at one common location, and internally distributed without need for further inspection.

Pros: One central 100% inspection point enables an efficient central clearinghouse for all goods designated for the Sterile Areas of the airport, provided that the site location is designed to support and accommodate the demand. One inspection center enables a more consistently controlled and secure process than managing various delivery and inspection locations throughout the airport. The big advantage with this best practice is related to logistics simplicity and better control of the process. Screened goods can then be delivered to any location within the airport without the need for further inspections and controlled areas. This is a big plus for the Cat 2 (and potentially Cat 3–4) airports because they likely will not require much upgrade in infrastructure to channel all deliveries through one inspection point, hence providing a more consistent and business friendly delivery and inspection portal.

Cons: A potential problem with a centralized 100% inspection area could develop if the queuing models are not prepared correctly or are inconsistent with the true volume of deliveries. Also, without appropriate lanes of entry or staffing, a centralized approach could experience delivery delays, idling trucks and requisite exhaust, and dissatisfied vendors. For the busy Cat X and 1 airports, this policy can impact investment expense in establishing a facility large enough to support delivery and inspection.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

2.4 People

2.4.1 Insider Threat Task Force

- Chaired by airport security; with local law enforcement and TSA; it is recommended that airports, where appropriate, consider airlines and other key airport stakeholders as participants
- Reviews mitigation strategies: employee inspections, background checks, and ACS history (access profiles)
- Uses advanced analytics via identity management technology to mine data in support of task force efforts
- Coordinates random inspections
  - Inspections are random and unpredictable
  - Times are based on data/history obtained via the ACS
- Inspections include LEOs and detectives
  - Detectives follow up on leads and tips
- Program includes:
  - Undercover detectives reviewing video and walking through various areas of the airport, including bag rooms, looking for suspicious behavior, following up on tips, and/or using data obtained from identity management system
  - Gate screening – Canine units are sent through hold rooms; detectives watch video, and if the canine hits on a passenger, they work to trace back video for any employee who may have been in contact with the passenger.

Pros: Establishing an Insider Threat Task Force brings together a team specifically focused on the threat and enforcement. It reduces variability in the process, and creates a Center of Excellence approach to defining the process, implementing the program, evaluating results, and continuously improving the inspection process. Enabling the Task Force with identity management tools further empowers the team to focus on areas of likely threats.

Such advanced technology for identity management and situational awareness can prove valuable to larger airports since they have so many access points and employees/contractors/vendors to monitor.

Cons: Potential problems with a task force approach is the added resources required to establish such an organization, and the commitment of law enforcement to sustain the program. At smaller airports with fewer badged personnel, the cost may not be justified, as access points can be monitored by existing resources.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	May be cost prohibitive	May be cost prohibitive

2.4.2 Insider Threat/Crime Suppression Group

- Use of Security Specialists
  - Review ACS and ID management data to look for card access use outliers; then use the detective unit to follow up
  - Review CCTV at doors and analytics for bags left, door alarm patterns, or loitering; if something is out of place, use detective unit/police/guard force to follow up as needed
- Active (anonymous) employee tip line
  - Encourage reporting of possible insider threats
  - Follow up with detective unit

Pros: A Crime Suppression Group brings similar benefits as those of the Threat Task Force; however, the objective is accomplished without sustained law enforcement involvement. This is a very reasonable alternative for smaller airports that have limited law enforcement resources and availability. An important component of this best practice is to have trained law enforcement or security guard staff provide interdiction. Also, creating a Crime Suppression Group made up of airport security staff is a viable option for Cat 2, 3, or 4 airports, which would have a lower threat risk than a Cat X or Cat 1 airport.

Cons: A potential issue with a Crime Suppression Group is the ability for the airport to fund it. The additional responsibilities associated with this group may impact utilization of it, especially in lieu of group members' other responsibilities, and likewise, could affect some operational costs as additional resources may be needed.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

2.4.3 Security Compliance Teams

- Audit employee inspections program, including oversight of credential/access anomalies
- Target various areas within the airport to expose insider threats and vulnerabilities
- Verify ACS portal issues and check on access portal violations
- Conduct random employee inspections and badge checks

Pros: A Security Compliance Team enables trained staff to conduct random inspections at predetermined areas of potential risk to the airport's key infrastructure assets. This offers consistency of inspections and the ability to observe trends that might not normally be identified. Not only can the

Security Compliance Team support the audit of the employee inspection program, but potentially all other Airport Security Program (ASP)-related compliance functions.

Cons: A consideration in establishing a Security Compliance Group is to ensure response mechanisms with appropriate law enforcement and security guard staff once an infraction is observed.

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	May be cost prohibitive

2.5 Other

2.5.1 Security Awareness Training and Outreach

- Conduct Security Awareness Programs for the airport community (including security-related posters, airport-employee-submitted artwork, and signage) in an active campaign to raise security awareness
    - Prizes and recognition for artwork
    - Artwork posted around airport
- Security Focus of the Month Campaign: One specific security topic highlighted in emails and other messaging.
- Ramp and Secured Area Challenge Program with reward incentives
- Conduct additional security focused training such as:
    - Workplace Violence
    - Active Shooter

Pros: An active Security Awareness Training and Outreach Program engages with the entire airport community and raises awareness of the indicators of out-of-compliance behavior, terrorism, and crime. This program reminds employees about maintaining best security practices. It helps to support the airport’s existing training programs, and highlights the importance of reporting suspicious activity.

Cons: There are essentially no cons. Cost may be the only consideration for some smaller airports in establishing a Security Awareness Training and Outreach Program

Cat X	Cat 1	Cat 2	Cat 3–4
✓	✓	✓	✓

REFERENCES

Final Report of the Aviation Security Advisory Committee’s Working Group on Airport Access Control. *Aviation Security Advisory Committee Report.* April 8, 2015.

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

ACS	Access Control System
ASP	Airport Security Program
AW	Aviation Worker
EAA	Excusive Area Agreement
ETD	Explosive Trace Detection
IC	Information Circular
LEO	Law Enforcement Officer
PARAS	Program for Applied Research in Airport Security
SD	Security Directive
SSCP	Security Screening Checkpoint
TDC	Travel Document Check

APPENDIX A: Survey Questions

I. Online Survey

Survey Introduction

Faith Group LLC is working on a Safe Skies' Program for Applied Research in Airport Security synthesis project (PARAS 0006), which is intended to create a reliable source of information for airports and air carriers to review methods of inspecting individuals that are in place and under consideration at airports within the United States. The synthesis considers airports of all sizes and complexities. The questions below (while generic) will help the project team gather much needed information for the synthesis. The survey portion of this project is a two (2) step process. In this first step, we are looking at obtaining as much information from as many airports as we can. In our second step, we will select from the airports who have responded and dive deeper into this subject matter with an onsite visit, teleconference and or face-to-face interviews.

For the betterment of the industry, we are looking for your uninhibited responses to these questions. Please feel free to elaborate on any response that you (or your staff) feel will best aid in describing and/or clarifying your airport and its current processes, including any proposed and future plans.

If your airport has implemented a successful program we would appreciate obtaining information about that program and any best practices you feel are appropriate. We believe that all of our questions (except for a potential request for a copy of any supporting Airport Security Plan ASP amendments) are non SSI. Faith Group team members currently hold active SIDA badges at multiple airports and can sign an SSI NDA should it be deemed necessary. Any data received will not be distributed in its “raw” form, and will be redacted to not violate SSI policies.

For the purposes of this survey, the terms “employee(s)” and “badge holders” are synonymous with one another and are purposefully used for specific data and information points the project team desires to obtain. When either of these two terms are used, they are meant to refer to any one individual, or group of individuals, who have an airport badge and access to secure areas of the facility.

Thank you in advance for your help and support.

Airport Respondent Information

1. Airport Information

- Airport Name
- Contact Name
- Title
- Email Address
- Telephone Number
- Airport Category

2. Badge Holder Information

- Total number of badge holders
- Number of Secure Identification Display Area (SIDA) badge holders

3. Employee Inspection Services

- Number of Airport Security Staff employees, including contractors, who perform employee inspections
- Briefly describe what inspection services the inspectors provide
- Briefly describe your Airport Security Staff employee’s role in inspections

4. Public to Sterile Access Points

- Total # of public to sterile access points in use?
- After the SD requirement became TSA ASP Amendment 12-03 was your airport been able to reduce the number of access points? (Yes/No)
- Has your airport been further able to reduce access points after the last Information Circular (IC) request? (Yes/No)

5. TSA Staffed Security Screening Checkpoints / Lanes

- Total # of checkpoints and Lanes. Please differentiate between checkpoints (Example: 3 checkpoints, 6 lanes, 8 lanes and 4 lanes)
- Are any lanes dedicated to badged employees? Please indicate how many lanes per checkpoint, if applicable.
- Are sterile-area-only employees required to use the TSA screening lanes?
- Please provide any additional background data you feel would be helpful.

Employee Screening Checkpoint or Inspection Location

The following questions are meant to outline and ascertain your airports process for badge holder screening or inspections. It is understood that Airports employ various methods and processes to meet the current federal requirements, and so all the following questions may or may not directly apply. Please fill out as many responses as are applicable to your current process.

6. Employee Inspection Overview

- Who manages the badge holder inspection location(s) or checkpoint(s)?
- If the TSA does not staff the inspection location, what kind of training program was implemented?
- Does your airport currently require a certain percentage (or number) of badge holders who enter the secure / sterile area to go through physical inspections? If so, what is that percentage (or number)?
- Does the inspection location or checkpoint use screening equipment, such as a walk-through metal detector, body scanner, or X-ray? If yes, did the airport provide the equipment?
- Do all airport badge holders, including airline employees, use the inspection location or screening checkpoint?
- Is the inspection location located directly at an access point to the secure area?
- Has the airport limited the number/size/style of bags that employees may bring into the secure/sterile areas? (Yes / No) If yes, what are the limitations?
- What facility related challenges have you experienced?
- Is the Screening checkpoint or inspection location(s) integrated into your Access Control System (ACS) and CCTV systems at the airport? (Used for badge checks, recording of inspections/screening, etc.)
- Has the airport changed and/or updated its rules and regulations to support employee inspections?
- (Yes / No) If yes, what specific changes were made?
- Did the Airport revise its ASP in support of employee inspections?
- (Yes or No) If yes, what was the ASP amendment?
- Does your airport management believe they have implemented a best practice associate with performing random employee inspections or screening?
- Please share anything else you may find relevant to this issue

7. Airline Process for Screening

- Do any of your air carriers have their own employee inspection facility and/or process?
- If yes, are security inspections required and or included in an Exclusive Area Agreement (EAA)?
- Can you please share with us the contact information for the group responsible for the EAA?

8. We understand that many airports do not have a formal designated location for employee inspections. If your airport does not have such a location, do you have plans to implement a formal badge-holder inspection location in the future? (Yes/No)

9. If plans do exist, can you please share the following details? (If no plans exist, please just answer N/A)

- Will all employees be required to use this inspection location (Yes / No)? If no, please describe your plan:
- Will more than one location be implemented?
- Will the location(s) be used for random or scheduled inspections?
- What is the schedule for implementation?
- What equipment will be utilized (if any)?
- Who will staff the location?
- Are there management or business challenges associated with establishing employee inspections at your airport? (Inspection avoidance, physical constraints, etc.)

Vehicle Gates, Ramp Inspections and Alternative Employee Inspection Measures

10. Vehicle Gates and Inspections

- Who currently provides inspection services at vehicle gates?
- Are all vehicles inspected?
- If no, what vehicles are exempt?
- Are all items within each vehicle inspected prior to entry into the AOA and/or SIDA?
- Does your airport use random inspection of vehicles and personnel at unmanned gates? If yes, what is the process?
- Are there management and/or business challenges associated with establishing vehicle inspections at manned or unmanned gates at the airport? If there are, can you elaborate further on these challenges?

11. Does your airport use random inspections of personnel, vehicles and goods on the ramp? If so, can you share the process?

12. Has your airport considered implementation of measures in addition to physical employee inspections aimed at addressing the insider threat? Please check whether these are Implemented— Planned—Not Planned for Implementation.

- Insider Threat Assessment Program
- Additional Internal Controls and Auditing
- Additional Signatory and Trusted Agent Training
- Risk-Based Security Programs
- Additional CCTV with Video Analytics
- Security Awareness Programs

Employee Inspection Round-Up

13. Please provide any additional relevant background information on your airport in support of the topic of employee inspections. (Airside access considerations, delivery of goods, escorting considerations, etc.)

14. Would your airport be willing to allow the Faith Group team to conduct a face-to-face interview with you and your staff? The interviews will include a more robust conversation on this topic in order to obtain an in-depth understanding of your airport's current processes and plans.

II. Airline Interview Survey

Faith Group LLC is working on a Safe Skies' Program for Applied Research in Airport Security synthesis project (PARAS 0006), which is intended to create a reliable source of information for airports and air carriers to review methods of inspecting individuals that are in place and under consideration at airports within the United States. The synthesis considers airports of all sizes and complexities.

We are looking for your support for this important project. Essentially we would like to obtain as much information from you and your Airline on the topic of Employee Inspections; what you are doing, what are you planning, and at what airports are these inspections and programs taking place. The questions below (while generic) are intended as a guide to help the project team gather much needed information for the synthesis. The goal of these questions is to enable a discussion on the topic.

If your Airline has implemented, or is in the process of implementing, an inspections program we would appreciate obtaining information about that program\ and the Airport(s) where the program has been implemented. We are looking for best practices in relation to the use and implementation of your processes and procedures, access control, intelligence gathering and use, technology, and any other best practice associated with your program.

While we believe that all of our questions are non SSI. Faith Group team members currently hold active SIDA badges at multiple airports and can sign an SSI NDA should it be deemed necessary. Any information obtained in our discussions or data received as part of the effort will not be distributed in its “raw” form. Data that is deemed to be SSI or potentially SSI will be so marked and controlled in accordance with 1520 in order not to violate SSI policies.

Thank you in advance for your help and support.

Airline Information #1

- Airline Name
- Contact Name
- Title
- Email Address
- Telephone Number
- Badge Holder Information
- Total number of badge holders

Number of Secure Identification Display Area (SIDA) badge holders

Employee Inspection Overview #1

- Does your Airline Currently have an Employee Inspection Program? Provide an overview of the Employee Inspection Program
- Who manages the inspection program?
- What airports have you implemented your inspections program / How is it run at each of these airports?

Employee Inspection Overview #2

- Does your Airline currently require a certain percentage (or number) of your employees / badge holders who enter the secure / sterile area to go through physical inspections? If so, what is that percentage (or number)?
- Does the inspection location or checkpoint use screening equipment, such as a walk-through metal detector, body scanner, or X-ray? If yes, did the airport provide the equipment?

Employee Inspection Overview # 3

- Has your Airline (or have any of your airports) limited the number/size/style of bags that employees may bring into the secure/sterile areas? (Yes / No) If yes, what are the limitations?
- What facility related challenges have you experienced?

Employee Inspection Best Practices #1

- Has your Airline implemented what it believes to be a BEST PRACTICE with regard to Employee Inspections? Please describe (implemented or planned)

Employee Inspection Best Practices #2

- Describe any types Technology which may have been implemented or planned

Employee Inspection Best Practices #3

- Describe any forms of Access Control which may have been implemented or planned

Employee Inspection Best Practices #4

- Describe any other systems/processes/procedures which may have been implemented or planned

Insider Threat and Employee Inspections #1

- Has your Airline considered implementation of measures in addition to physical employee inspections aimed at addressing the insider threat? Please Describe your inside Threat Program (if implemented or planned)

Insider Threat and Employee Inspections #2

- Please describe what Additional Internal Controls and/or audits have been implemented and/or planned

Risk Based Security Programs

- Please Describe what Risk-Based Security Program(s) have implemented and/or planned

Security Awareness Programs

- Please describe what Security Awareness Program(s) which have been implemented and/or planned in support of Employee Inspections**:**

Intelligence Gathering In Support of Security and the Insider Threat

- Please Describe what programs your Airline has implemented / or plans to implement with regard to Intelligence Gathering In Support of Security and the Insider

APPENDIX B: Data Gathering

The Team determined that the most appropriate tool for the online survey would be a well-known existing product. The product utilized for this effort was Survey Monkey, which enables the users to mine the data received for detailed information, trends, analysis and ease of reporting. The intent of the online survey was to generate data that would be useful in capturing the state of the industry with regard to employee inspections and to set the stage for face-to-face and/or telephone interviews with those airlines and airports that have a more mature employee inspection process in-place.

The Team experienced difficulty in obtaining survey results and establishing the interview schedule. The individuals the Team wanted to speak with were extremely busy. The feedback received from the industry was that there were several interview and survey requests ongoing across the whole airport industry. This, coupled with the release of additional revisions to SDs and ICs; the need for airports to submit mitigation plans; and other trade, professional, and research-based organizations performing active surveys, made it difficult for the industry professionals to set aside time in their day-to-day requirements in order to fully respond to our survey or participate in interviews.

Survey

In preparation for the survey, the Team researched and selected airports to contact, the number and complexity of which represented a cross-section of airports that have either established an employee inspection program or have an emerging program.

Approximately 180 contacts were provided the survey link. A total of 30 survey responses were received. Of those, 28 were unique airport responses and 13 surveys were completed in their entirety. Additional outreach took place, which resulted in a total of 19 detailed airport responses and 2 detailed airline responses to make up this synthesis report. Our Team made multiple efforts to follow up with those airports that responded to the survey but did not provide data or respond to every question. The Team also reached out to additional airports who were on the initial list but who had not responded to the survey at all. Although the number of initial responses was fewer than desired, some very good information was received, which provided a basis for the face-to-face and interview discussions.

Interview

The Team utilized the initial responses from the online survey to create a plan to conduct face-to-face and/or telephone discussions. Based on the Team’s follow up to the initial survey, two additional telephone interviews with airports that could not complete the survey in the initial time frame were scheduled. These interviews provided more specific details and insight into their processes, challenges, and best practices.

Of the 13 airports who completed the surveys, 11 indicated that they would participate in face-to-face or telephone interviews; through continued outreach, a total of 17 airports and 2 airlines participated.

Summarized results from the surveys and interviews are contained in Section 1 of this report. Best Practices are described in Section 2.

AUTHOR ACKNOWLEDGMENTS

Airlines and airports are facing a continuing and evolving threat posture from individuals or terrorist organizations wishing to inflict harm against our country’s critical infrastructure. Threatened areas include those of high public access, high visibility, and locations that, if compromised, would significantly disrupt our nation’s way of life, cause economic losses, and create a sense of fear among its citizens. It has become increasingly apparent that ‘insiders’ are another potential gateway for individuals or organizations to inflict harm. One way to confront the reality of the insider threat is to perform employee inspections and additional vetting. It is the airports, with their airline partners, who have addressed the regulatory requirements, operational needs, and local and national political challenges to develop and implement such processes. Acknowledgments go to the following airports and airlines that participated in this endeavor to provide the industry with much needed information:

- American Airlines
- Dallas/Fort Worth International Airport
- Delta Air Lines
- Denver International Airport
- Des Moines International Airport
- Fairbanks International Airport
- Fort Lauderdale–Hollywood International Airport
- General Mitchell International Airport
- Hartsfield–Jackson Atlanta International Airport
- Kansas City International Airport
- Los Angeles International Airport
- Oakland International Airport
- Philadelphia International Airport
- Phoenix Sky Harbor International Airport
- Pittsburgh International Airport
- Portland International Airport
- Sacramento International Airport
- San Antonio International Airport
- Seattle–Tacoma International Airport
- Salt Lake City International Airport