THE

PUBLIC-PRIVATE

ANALYTIC EXCHANGE PROGRAM

Aviation Insider Threat Team 2017

Aviation Insider Threat: What We Know, Our Findings, and What We Recommend

2017

Protecting the Aviation Industry against the threat from insiders is everyone's responsibility. As we have seen through a multitude of past cases, insiders will continue to seek to challenge security countermeasures, exploit potential vulnerabilities, and increase their knowledge of security procedures for nefarious purposes. Through a combined effort, this Aviation Insider Threat Working Group seeks to leverage the best practices of the Private Sector and Federal Government in efforts to establish a baseline standard in identifying and reporting insider threat. This standard will look to achieve consistent insider threat mitigation and awareness messaging to employees within the aviation ecosystem and perhaps the traveling public.

Table of Contents

Key Intelligence Questions

- Key Intelligence Questions (KIQ) for the Aviation Insider Threat……. 2

What We Know

- Findings.…… 3
- Who is the Aviation Insider? ……. 3
- What are the Types of Intent Behind an Insider?……... 3
- What are the Types of Insider Threat? ……..... 4
- Past Examples of Insider Threats in the Aviation Sector ……... 4-5
- Behavioral Indicators Identified in Past Insiders …….. 6

Our Findings

- Insider Threat within the Aviation Industry: Different Definitions – Same Meaning …… 7
- Survey Results ……... 7-9

What We Recommend

- Public Sector Recommendation ……. 10
- Private Sector Recommendation ……... 10-11
- Public/Private Sector Recommendations ……...11-13

Team Participants……. 14

Sources ……...15-16

From the onset, the AEP Aviation Insider Threat Team's goal has been to address as many of the DHS provided Key Intelligence Questions (KIQs) as possible through this paper to include the following aspects: providing what we already know as professionals working within the aviation sector in regards to the insider threat; what we found out through our collaboration as professionals, through a survey of the aviation sector and through our research trip; and through our recommendations for both private and public sector partners to combat insider threat.

1. How are potential aviation insiders identified and recruited by criminal organizations? How are they recruited by terrorist groups? How have recruitment techniques evolved to utilize anonymous means to mask the recruiter and the individual being recruited?
2. What external factors (social media exploitation, open source articles, media leaks, etc.) would lead to the successful extorting of an individual to become an insider?
3. What indications are there of criminal and terrorist organizations infiltrating the aviation sector?
4. What are the characteristics of a criminal insider? What are the characteristics of a terrorist insider including both supporters and operatives? What are the motivational differences between criminal and terrorist insiders?
5. What indicators do criminal and terrorist insider's exhibit?
6. What are public and/or private best practices for identifying insider threats?
7. What mechanisms exist for observers of insider threat indicators to report suspicious behavior to federal investigators? What roadblocks exist for reporting of suspicious behavior to federal investigators? Do current reporting procedures protect and encourage an individual who is reporting the suspicion of an insider threat or discourage reporting?
8. What are public and/or private mitigation measures for insider threats? What type of predictive analytics and vetting practices are being utilized or developed to support insider threat mitigation measures? What is the aviation industry doing to better promote information security?
9. How can public and/or private organizations improve reporting of suspicious activity by aviation insiders to federal investigators?
10. Within the aviation sector, what are some examples of complacency to security policies that an insider can leverage to facilitate illicit activity?

WHAT WE KNOW

Findings:The Analytic Exchange Program (AEP) Aviation Insider Threat Team believes with a high degree of probability, that insiders pose a great risk to the safety and security of the aviation industry by challenging security countermeasures, exploiting potential vulnerabilities and increasing their knowledge of security procedures for nefarious purposes. These findings are made with significant confidence based upon past incidents, survey results related to the insider threat, and information provided by the public and private sector during the course of the study.

Who is the Aviation Insider?

Potential Insider Threats within the Aviation Industry include a wide variety of individuals involved with the aircraft and passengers, including, but not limited to, the following categories:

- Airline employees
- Concession and restaurant employees
- Cleaning and catering crews
- Construction and maintenance crews
- Law enforcement, military and/or security personnel
- Taxi cab, shuttle bus and/or other transportation specialists
- Current and/or former TSA employees
- Current and/or former contract government employees
- Air Traffic Controllers

What are the Types of Intent Behind an Insiders Act?[i]

Historically, the insider threat is considered to be a malicious insider or group who seeks to do harm; however, it is important to remember that the insider threat can be unintentional as well. Personality, behavioral, and lifestyle indicators may alert us to the malicious insider; however, the unwitting or complacent insider could go undetected by peers and supervisors.

- **Malicious:** Insider seeks to aid or conduct an act that is malicious and intentional in nature to cause damage
- **Complacent**: Insider takes a lax approach to policies, procedures, and potential security risks
- **Unwitting**: Insider is not aware of security policies, procedures and protocols which expose the organizations/agency to external risks.

What are the Types of Insider Threats?[ii]

The insider threat to the aviation sector spans across all realms of the threat vector to include cyber, criminal, and terrorism. Some of the more notable examples of aviation insider threat across the globe include terrorism/sabotage, security compromise, and physical property theft.

Terrorism	Use of insider access to facilitate an act of violence as a means of disruption or coercion for political purposes.
Espionage	Use of insider access to obtain sensitive information for exploitation.
Security Compromise	Use of insider access to facilitate and circumvent security controls.
Sabotage	Use of insider access to destroy equipment or materials.
Physical Property Theft	Use of insider access to steal material items.
Information/Intellectual Property Theft	Use of insider access to steal information or intellectual property.
Workplace Violence	Use insider access to conduct violence in the workplace.

Past Examples of Insider Threats in the Aviation Sector:

Terrorism/Sabotage (United Kingdom): In early 2011, a former British airline employee, acting under orders from a "major terrorist planner", was convicted of four counts of preparing acts of terrorism for offering to help a foreign terrorist organization (FTO) disrupt or damage airline computer systems. The airline employee bragged to the FTO that he had access to the airline's computer systems and could erase data that could cause massive disruption and financial loss for the airline. The airline employee also suggested to the FTO that he knew two individuals that may be willing to assist, one worked in baggage handling and the other in security. The airline employee and his brother turned towards the FTO's world view and began following radical Islamist thinking over the internet and in study groups.[iii]

Terrorism (Wichita, KS). In mid-December 2013, a former airport worker was arrested and charged with attempted use of a weapon of mass destruction, maliciously attempting to damage and destroy by explosive, and attempting to provide material assistance to a FTO. The individual, an avionics technician with Secure Identification Display Area badge access to Wichita Mid-Continent Airport, was taken into custody after he allegedly armed what he believed to be an explosive device and attempted to open a security access gate. During the investigation, the individual allegedly engaged in, among other things, pre-operational surveillance, photographing gate access points, researching flight

schedules, and assisting in the acquisition of vehicle-borne improvised explosive device components and construction of an explosive device.[iv]

Security Compromise (Atlanta, GA): In late 2014, an airport employee was arrested and charged with trafficking firearms and entering secure areas of a US airport in violation of security requirements. The complaint alleges that the employee "repeatedly evaded airport security with bags of firearms, some of which were loaded". The employee then passed the guns off to an accomplice who transported them as carry-on luggage to New York, where they were illegally sold."[v]

Terrorism (Somalia): In early 2016, shortly after takeoff, an explosion occurred onboard an aircraft traveling from Somalia. Somali intelligence officials say two airport workers handled a laptop containing a bomb that later exploded in a passenger plane. A video shows one airport worker handing the laptop to another employee. The two then hand the laptop over to a man who was later killed when the laptop exploded.[vi]

Physical Property Theft (Denver, CO): In late August 2016, an airline employee was arrested and charged with one count of felony theft for allegedly stealing $130,000 worth of jewelry from a passenger's bag at a U.S. airport. Video from the airport's surveillance system appears to show the employee "taking possession of the ... cosmetic case[vii]... and intentionally wrapping the case with a white piece of [printer] paper," at the gate, according to the statement of probable cause provided by the District Attorney's office.[viii]

Security Compromise (San Juan, Puerto Rico): In early February 2017, a federal grand jury returned a superseding indictment against twelve defendants – to include six federal government employees, airport security personnel, and ramp employee – who have been charged with conspiracy to possess with the intent to distribute cocaine. According to the indictment, during the course of the conspiracy, the defendants smuggled suitcases, each containing cocaine, through the TSA security system at the Luis Muñoz Marín International Airport (SJU) and then onto airplanes without detection. Sometimes as many as five mules were used on each flight, with each mule checking-in up to two suitcases. From 1998 through 2016, the defendants helped smuggle approximately 20 tons of cocaine through SJU.[ix]

Behavioral Indicators Identified in Past Insiders

Identifying behavioral indicators and educating employees is key. In reviewing previous insider cases, the Aviation Insider Threat Team finds that indicators, whether they be physical/technological/financial, were present that could have exposed the insider to detection. However, for a multitude of reasons, co-workers did not notify their chain of command or law enforcement of the suspicious behavior(s). In part, this was due to a lack of training or awareness of employees on potential indicators. The Aviation Insider Threat Team consulted several sources and compiled a list of some of the most common indicators.[x]

Potential Indicators of an Insider Threat within the Aviation Industry[xi, xii]	
Significantly altered appearance	Burns on hands or body; chemical bleaching of skin
Displays of nervous or secretive behavior; sweating; lack of eye contact	Apparent monitoring of access points
Body language/movement consistent with "photo panning" with a hidden camera	Avoidance of security cameras
Requests to work alone and/or on unsupervised shifts	Facilitation of unauthorized visitors; at the airport in uniform on days off
Threatening comments/threats of violence against the United States or individuals	Allows access badge sharing and "piggy backing" at security gates and doors
History of criminal activity and arrests	Disregard for security policies
Enthusiastic interest in security matters outside the scope of his/her duties	Working unusual hours without authorization
Misusing credentials	Suspicious foreign contacts or travel, including via internet and social media
Unexplained or sudden wealth	Misusing cyber systems
Conducting unauthorized searches	Withholding or misreporting information necessary for counterterrorism efforts
Efforts to conceal the transfer of money or other financial resources into or out of the United States	Participation in transshipment of illicit goods or persons
Colluding with criminal enterprises to facilitate access to the aviation domain	[intentionally left blank]

Potential Job-Specific Insider Threat Indicators[xiii,xiv]		
On Aircraft & On Ramp Providers	**In-Terminal Providers**	**Outside-terminal Providers**
Access Abuse	Additional access sought	Overly willing to run sensitive routes and pick ups
Loitering outside of duty areas	Loitering outside of duty areas	Additional access sought
Arrival or departure with unusual items or luggage	Theft of official vehicles, uniforms, identification, and access cards	Extended parking in a restricted area
Cargo theft and other criminal activity	Unusual inquires made about sterile side security procedures	Surveillance of persons or vehicles passing through

OUR FINDINGS

Insider Threat within the Aviation Industry: Different Definitions – Same Meaning
The definition of "insider" can vary depending on who you work for and whether you are in the private sector or in the public sector, but the AEP Aviation Insider Threat Team concludes the meaning is the same. For example, the below features definitions that are similar in nature, but different—regardless, the meaning is the same:

> **US Airline:** According to a US Airline, the insider threat is a current or former employee, contractor, vendor, or other business partner, who has or had authorized access to an organization's information, abilities, products, or supply chain. This knowledge or access is then misused to negatively affect the organization or to do harm to the public.[xv]
>
> **Private Sector Company**: According to a private sector company, insiders are persons who have the potential to harm an organization for which they have inside knowledge or access. An insider threat can have a negative impact on any aspect of an organization, including employee and/or public safety, reputation, operations, finances, national security and mission continuity.[xvi]
>
> **TSA:** TSA defines insider threat as an individual with the intent to cause harm and with access and/or insider knowledge that would allow the individual to exploit vulnerabilities of the nation's transportation systems. In the aviation domain, this potentially includes current or former TSA employees and contractors, airline employees, cleaning and catering crews, construction and maintenance workers, law enforcement, military and security forces, taxi cab drivers or transportation specialists, or other airport personnel who have access and/or insider knowledge.[xvii]
>
> **FBI:** "'Insiders,' which are corrupt employees who exploit their credentials, access, and knowledge of security procedures."[xviii]

Survey Results Overview:

The survey was comprised of 160 participants from 16 different sectors of the aviation industry. The majority of respondents were affiliated with international air carriers, non-federal airport-based law enforcement, domestic air carriers, and airport governance. Survey results revealed 54% of the responding organizations currently have an insider threat training or awareness program (training includes; classroom handouts, posters, computer-based modules, books) specific to the aviation industry and 46% of the respondents do not have a program in place.

Aviation Insider Threat Training Programs

For those organizations that currently have an aviation-focused insider threat training or awareness program implemented; the top 50% or more reported having the following topics in their program:

- Badge/access activity monitoring;
- Recurring background/criminal check on employees;
- Employee security screening/bag checks (random or daily);
- Central system for reporting suspicious or anomalous behavior;
- CCTV monitoring;
- Classroom training/briefs, guest speakers;
- Computer Based Training (CBT); and/or
- Incident response protocols implemented.

Other program initiatives include:

- Computer activity monitoring;
- Handouts/Booklets;
- Posters;
- Emails to workforce addressing insider threat;
- Employee bag restrictions (clear, no backpacks, etc.);
- Fines (no badge displayed, access violation);
- Reward program for reporting suspicious activity/violations of colleagues;
- Formalized insider threat policies and procedures for the organization; and/or
- Suggestion boxes.

The primary areas of focus addressed in insider threat training programs are: terrorism, suspicious activity, and active shooter.

Computer Based Training (CBT)

31% of organizations currently provide a CBT module addressing the aviation insider threat; of those organizations providing a CBT module, the majority of training (55%) lasts 15 minutes or less, followed by 60 minutes and 30 minutes – there is no CBT standard.

When asked how long CBT training should last; majority responded with 30 minutes, and 15 minutes or less.

The majority of CBT content includes:

- ✓ Videos;
- ✓ Defining the threat;
- ✓ Personal actions to take during an attack by an insider;

- ✓ How to identify suspicious activities among coworkers and employees;
- ✓ Why everyone should care, "it won't happen here"; and/or
- ✓ Terrorist insiders.

When asked what areas or content employees would like to see covered in a CBT, the majority of answers matched the above (content already included in CBT) plus additional content:

- ✓ A short quiz to reinforce key points;
- ✓ What happens after a suspicious coworker is reported to management, "How come I haven't heard anything, did the authorities drop the ball on this?";
- ✓ Criminal insider activity (e.g., theft, smuggling); and/or
- ✓ The cyber insider.

Training Overview

- ✓ Training is mostly provided to employees via CBT, classroom/briefing, and poster/signage; only 25% provide scenarios/exercises and a booklet/manual.
- ✓ On average 81% of employees receive insider threat training yearly and 13% receive training semi-annually.
- ✓ The most effective training method reported was classroom/briefing, poster/signage, and CBT, while the most effective method for conveying the insider threat at organizations is CBT (51%), followed by scenarios/exercises, and classroom/briefing.
- ✓ The least effective training method reported was booklet/manuals and posters/signage, while the least effective method for conveying the insider threat is via booklet/manual (45%) and postage/signage (27%).
- ✓ Most employees would like to receive insider threat training via CBT, classroom/briefing, and scenarios/exercises.
- ✓ Seventy-three percent of respondents indicated their organizations would be "more than likely", "extremely likely" or "definitely would," use Aviation Insider Threat CBT training if provided by the U.S. Government.

WHAT WE RECOMMEND

Public Sector Recommendations:

Recommendation 1: Every business unit/office has a role to play in mitigating the insider threat within an agency/organization. The AEP Aviation Insider Threat Team recommends the creation of a cross-functional governance committee to support the building and maintenance of an insider threat program within the aviation industry, with participation by all business units/offices. Essentially, this would be the creation of a funded Insider Threat Program Office that would coordinate activities between physical security, HSPD-12 / Credentialing HR and Internal Investigations. This office would be a coordination body designed to proactively educate and implement sound effective Insider Threat Programs across the government and aviation sector.

- The aforementioned cross-functional governance committee could be established and enhanced by holding an Aviation Security Insider Threat Summit similar to the 2016/2017 Public Area Security Summit led by TSA. In similar fashion, the Aviation Security Insider Threat Summit would bring together a group of industry, government, academic and international, and public officials to devise a strategy to share information, prevent attacks and protect infrastructure from emerging insider threats within the aviation sector.[xix]

Private Sector Recommendations:

Recommendation 1: The AEP Aviation Insider Threat Team recommends highlighting the insider threat and the potential consequences to executives to obtain their support to either create, enhance policy, or establish a program office to champion the insider threat program. In order to accomplish this, we recommend each organization:

- Highlight the need to deploy insider threat training to the workforce, describing what an insider threat is, what indicators to look for, and how to report an insider threat;
- Highlight the need to inform employees that the organization has a right to monitor their activities in the workplace and on the organization's network;
- Highlight the need to periodically update, communicate, and collaborate within each business unit/office on issues that arise both internally and externally on insider threat policy; and
- Highlight past examples within the aviation industry and the damage they cause or could have caused (physical and financial).

Recommendation 2: The AEP Aviation Insider Threat Team recommends each organization build an insider threat program around their "crown jewels." In order to accomplish this, we recommend each organization:

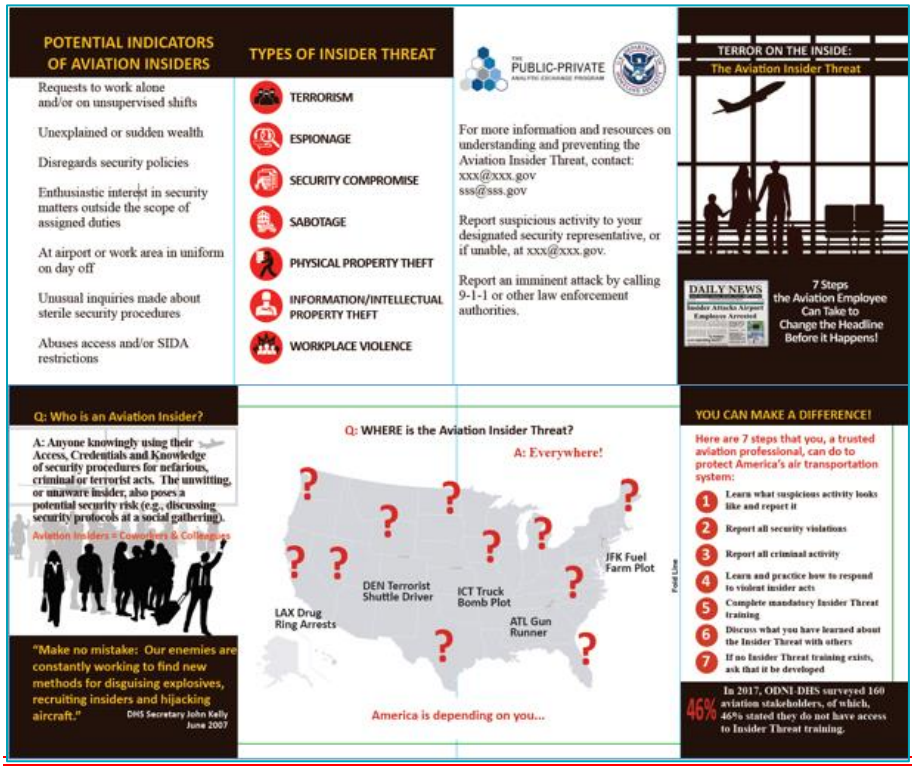
- Prioritize their assets[xx] to determine which assets make up the "crown jewels";
- Look at who has access to those critical assets;
- Decide what additional monitoring or scrutiny those individuals with key access will need to go through; and
- Determine the best way to enact an insider threat program designed to protect the crown jewels.

Public/Private Sector Recommendations:

Recommendation 1: Considering the definition of an "insider" can vary, a one-size fits all approach may not be a viable option[xxi]. For this reason, the AEP Aviation Insider Threat Team recommends the creation of virtual Aviation Insider Threat "Center of Excellence" information sharing platform. To be successful, this platform must be endorsed by a cross-functional governance committee to include, but not limited to the following: Federal Bureau of Investigation (FBI), Transportation Security Administration (TSA), Airport Law Enforcement Agencies Network (ALEAN), Air Line Pilots Association (ALPA), and American Association of Airport Executives (AAAE). The AEP Aviation Insider Threat Team recommends this virtual information sharing platform have the following characteristics:

- The site must be set up as a SharePoint, an internal information sharing platform which may be open sourced and cloud based in its architecture type for aviation industry security users only.
- Users of the site must be Sensitive Security Information (SSI) approved.
- Users must be able to house or maintain documentation at the SSI level, posted and/or stored.
- Government agencies, in particular the FBI and TSA, need to have the ability to share unclassified and up to SSI documents such as PowerPoints, brochures, assessments, and posters that can help private organizations derive information to assist and in some cases create an insider threat program to tailor to their specific needs and/or concerns.
- Each agency/organization must have the ability to post information and/or references.
- The website must be password protected and have SSL and NIST security standards.
    - Key staff in private industry who have access should go through a public trust background investigation.

Recommendation 2: The AEP Aviation Insider Threat Team created a one-page "Threat Pocket Reference Guide" and poster to educate employees in the aviation sector. Specifically, the reference guide includes potential indicators highlighted at the unclassified level in reports by the FBI and TSA. The AEP Aviation Insider Threat Team recommends this guide and poster be released throughout the aviation industry to educate their workforce on the threat of insiders and/or to assist the private organization in developing their own insider threat program.


POTENTIAL INDICATORS OF AVIATION INSIDERS
Requests to work alone and/or on unsupervised shifts
Unexplained or sudden wealth
Disregards security policies
Enthusiastic interest in security matters outside the scope of assigned duties
At airport or work area in uniform on day off
Unusual inquiries made about sterile security procedures
Abuses access and/or SIDA restrictions
TYPES OF INSIDER THREAT
TERRORISM
ESPIONAGE
SECURITY COMPROMISE
SABOTAGE
PHYSICAL PROPERTY THEFT
INFORMATION/INTELLECTUAL PROPERTY THEFT
WORKPLACE VIOLENCE
PUBLIC-PRIVATE
For more information and resources on understanding and preventing the Aviation Insider Threat, contact:
xxx@xxx.gov
sss@sss.gov
Report suspicious activity to your designated security representative, or if unable, at xxx@xxx.gov.
Report an imminent attack by calling 9-1-1 or other law enforcement authorities.
TERROR ON THE INSIDE:
The Aviation Insider Threat
DAILY NEWS
7 Steps the Aviation Employee Can Take to Change the Headline Before it Happens!
Q: Who is an Aviation Insider?
A: Anyone knowingly using their Access, Credentials and Knowledge of security procedures for nefarious, criminal or terrorist acts. The unwitting, or unaware insider, also poses a potential security risk (e.g., discussing security protocols at a social gathering).
Aviation Insiders = Coworkers & Colleagues
"Make no mistake: Our enemies are constantly working to find new methods for disguising explosives, recruiting insiders and hijacking aircraft."
DHS Secretary John Kelly
June 2007
Q: WHERE is the Aviation Insider Threat?
A: Everywhere!
DEN Terrorist Shuttle Driver
ICT Truck Bomb Plot
JFK Fuel Farm Plot
LAX Drug Ring Arrests
ATL Gun Runner
America is depending on you...
YOU CAN MAKE A DIFFERENCE!
Here are 7 steps that you, a trusted aviation professional, can do to protect America's air transportation system:
1 Learn what suspicious activity looks like and report it
2 Report all security violations
3 Report all criminal activity
4 Learn and practice how to respond to violent insider acts
5 Complete mandatory Insider Threat training
6 Discuss what you have learned about the Insider Threat with others
7 If no Insider Threat training exists, ask that it be developed
46%
In 2017, ODNI-DHS surveyed 160 aviation stakeholders, of which, 46% stated they do not have access to Insider Threat training.


AVIATION
INSIDER THREAT
NOT ON
OUR
WATCH
As an aviation employee, the responsibility for ensuring America's aviation system functions in a safe and effective manner falls on you. Together, we are responsible for all travelers. Every day, the traveling public relies on us to be vigilant, to report suspicious activity, and to ensure that everyone makes it home safe.

Recommendation 3: The AEP Aviation Insider Threat Team recommends each agency/organization develop a social media strategy/training to help protect themselves from the unwitting insider, including but not limited to:

- The worker who posts about his/her job responsibilities – this is likely done so harmlessly but the impact can be devastating.
  - These posts make the worker susceptible to recruitment by criminal/terrorists/foreign entities to smuggle and/or avoid established security protocols.
- The baggage handler who routinely posts about being at work and how much he hates his co-workers/his job.
  - These posts may place the employee in a position to be compromised or recruited by criminals, terrorists, or foreign entities.

Unfortunately, there is no 100% solution to completely eliminate insider threat. The insider threat constantly evolves – therefore the insider threat program should be maintained and adjusted to industry trends, indicators and threats.

Private Sector Project Team:

- Hyatt Hotels Corporation
- Allied Universal Security
- Boeing
- Citizant
- MITRE Corporation
- San Diego International Airport
- UPS

Public Sector Project Team:

- FBI
- DHS/TSA/OIA
- Port Authority of New York & New Jersey

Project Champions:

- DHS/TSA

[i] This section was based on information found in: *Source: Website; Aci-Na.org; "Deloitte - Insider Threat Mitigation: Considerations for Building an Industry Leading Insider Threat Program"; http://aci-na.org/sites/default/files/aci_deloitte_presentation.pdf; accessed on 24 July 2017; "Deloitte" is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, tax, and related services to select clients.*

[ii] This section was based on information found in: *Source: Website; Aci-Na.org; "Deloitte - Insider Threat Mitigation: Considerations for Building an Industry Leading Insider Threat Program"; http://aci-na.org/sites/default/files/aci_deloitte_presentation.pdf; accessed on 24 July 2017; "Deloitte" is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, tax, and related services to select clients.*

[iii] Online news article; Steve Swann; BBC.com; "Rajib Karim: The Terrorist inside British Airways"; 28 February 2011; http://www.bbc.com/news/uk-12573824; accessed on 20 July 2017; BBC is a reputable news syndicate.

[iv] Website; Homeland.House.gov; "Subcommittee Hearing: A Review of Access Control Measures at Our Nation's Airports"; 03 February 2015; https://homeland.house.gov/hearing/subcommittee-hearing-review-access-control-measures-our-nation-s-airports/; accessed on 8 August 2017; Source is the Homeland Security Committee.

[v] Online Press Release; Department of Justice, US Attorney's Office for the Northern District of Georgia; "Baggage Handler at Hartsfield-Jackson Airport Arrested for Smuggling Guns Into Airport by Evading Security"; 23 December 2014; https://www.justice.gov/usao-ndga/pr/baggage-handler-hartsfield-jackson-airport-arrested-smuggling-guns-airport-evading; accessed on 20 July 2017; Source is the US Department of Justice.

[vi] Online news article; Robyn Kriel and Faith Karimi; CNN; "Airport workers seen with laptop used in Somalia in-flight jet blast"; 08 February 2016; http://www.cnn.com/2016/02/07/africa/somalia-airplane-explosion-video/; accessed on 20 July 2017; CNN is a reputable news syndicate.

[vii] According to the article, the cosmetics case contained the passenger's jewelry.

[viii] Online news article; Becky Perlow; ABC News; "United Airlines Employee Allegedly Steals $130K in Jewelry From Passenger"; 31 August 2016; http://abcnews.go.com/US/united-airlines-employee-allegedly-steals-130k-jewelry-passenger/story?id=41773004; accessed on 20 July 2017; ABC is a reputable news syndicate.

[ix] Web site; justice.gov; Twelve Current and Former TSA and Airport Employees Indicted for Smuggling Approximately 20 Tons of Cocaine; 13 February 2017

[x] **Note:** There may be legitimate and lawful reasons why these indicators are observed. Each of these activities may have innocent explanations. We are asking you to report suspicious behavior to be examined by law enforcement professionals in a larger context to determine whether there is a basis to investigate. Some of the behaviors listed above may be rooted in cultural/ethnic patterns or norms, and would not be considered suspicious in that context; however, the behavior could constitute an indicator if it is a departure from the suspected insider's established pattern of behavior. The activities outlined on this handout are by no means all-inclusive, but have been compiled from a review of terrorist events over several years. *It is important to remember that just because someone's speech, actions, beliefs, appearance, or way of life is different does not mean that he or she is suspicious.* – *Web site; FBI.gov; "Potential Indicators of Terrorist Activities Related to Airport Service Providers"; 20 March 2012;*

[xi] Web site; FBI.gov; "Potential Indicators of Terrorist Activities Related to Airport Service Providers"; 20 March 2012; http://attleboropoliceorg.c.presscdn.com/wpcontent/uploads/2015/07/MassGatheringsV2.pdf; accessed on 20 July 2017; The FBI is an agency within the United States Department of Justice.

[xii] Transportation Security Administration; Office of Intelligence and Analysis; Insider Threats to Aviation and Potential Indicators; 15 June 2016 – on SAGE

[xiii] Web site; FBI.gov; "Potential Indicators of Terrorist Activities Related to Airport Service Providers"; 20 March 2012; http://attleboropoliceorg.c.presscdn.com/wpcontent/uploads/2015/07/MassGatheringsV2.pdf; accessed on 20 July 2017; The FBI is an agency within the United States Department of Justice.

[xiv] Transportation Security Administration; Office of Intelligence and Analysis; Insider Threats to Aviation and Potential Indicators; 15 June 2016 – on SAGE

[xv] Email Communication; US Airline; Internal Definition of Insider Threat; 24 July 2017; Email communication from threat team member.

[xvi] Website; Aci-Na.org; "Deloitte - Insider Threat Mitigation: Considerations for Building an Industry Leading Insider Threat Program"; http://aci-na.org/sites/default/files/aci_deloitte_presentation.pdf; accessed on 24 July 2017; "Deloitte" is the brand under which tens of thousands of dedicated professionals in independent firms throughout the world collaborate to provide audit, consulting, financial advisory, risk management, tax, and related services to select clients.

[xvii] Transportation Security Administration; Office of Intelligence and Analysis; (U//FOUO) Insider Threats to Aviation and Potential Indicators; 15 June 2016 – on SAGE

[xviii] Federal Bureau of Investigation – National Joint Terrorism Task Force; Transportation Security Programs; Seeking Information – Insider Threat (Transportation); April 2014 – on SAGE

[xix] Transportation Security Administration; Public Area Security National Framework; May 2017

[xx] Assets may be prioritized based on various criteria such as a business driver, cost, national security, safety, etc.

[xxi] Additional information on Industry Insider Threat Information and Resources may be found at: http://www.dss.mil/it/index.html