PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0026 March 2021

# Insider Threat Mitigation at Airports

**National Safe Skies Alliance, Inc.**

Sponsored by the Federal Aviation Administration

**Salus Solutions**

www.Salus.Solutions

## 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 ASSIST (Airport Security Systems Integrated Support Testing) 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 POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), 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 of 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 PARAS Program Manager*

### PARAS 0026 PROJECT PANEL

**Martina Benedikovicova** *Charlotte Douglas International Airport*
**Frank Capello** *Broward County Aviation Department*
**Colleen Chamberlain** *American Association of Airport Executives*
**Scott Creager** *Port of Portland*
**Sarah Demory** *Phoenix Sky Harbor International Airport*
**Michele Freadman** *Massachusetts Port Authority*
**Tracy Fuller** *ACTS – Aviation Security, Inc.*
**David Hornsby** *Dallas Fort Worth International Airport*
**Lisa Rousseau** *Port of Seattle*
**Timothy Tyler** *Metropolitan Washington Airports Authority*
**Jon "JT" Taylor** *Dallas Fort Worth International Airport*
**Serge Potapov** *Ex-Officio, Transportation Security Administration*

## AUTHOR ACKNOWLEDGMENTS

The research team would like to thank the airport administrators, vendors, and concessionaires who took time out of their busy schedules to help make this guidebook robust and useful to airports of all sizes. It is only through the support of airports that Safe Skies is able to continue to provide the aviation industry with valuable research on practical airport related topics. Finally, the research team wants to thank the panel of volunteers who lent their expertise and time to ensure the guidebook would be useful and applicable.

## CONTENTS

## TABLES & FIGURES

# HOW TO USE THIS GUIDEBOOK

This guidebook is an all-encompassing source for information on insider threat mitigation at airports.

To use this document most effectively, begin by reviewing the table of contents to get an overview of the information in the guidebook, and to identify the sections that are especially relevant to your role and responsibilities at the airport.

You can also use the information in this guidebook to develop other materials for your airport's needs, such as presentations for training, and information cards and other handouts with specific information for various roles within your organization.

In the appendices of the guidebook are several additional sources, including checklists for planning and reference material for more information.

Acknowledging the importance of the work accomplished by the Aviation Security Advisory Committee (ASAC), this guidebook aligns with the six focus areas discussed in the ASAC report, "Review of TSA's Insider Threat Advisory Group Findings." Those focus areas are:

1. Threat Detection, Assessment, and Response
2. Aviation Worker Vetting and Evaluation
3. Aviation Worker Screening and Access Control
4. Training and Engagement
5. Information Sharing
6. Governance and Internal Control

Legend boxes with reference information have been placed in the sections throughout this guidebook that correspond to specific sections of the ASAC report.

## PARAS ACRONYMS

| | |
|---|---|
| **ACRP** | Airport Cooperative Research Project |
| **AIP** | Airport Improvement Program |
| **AOA** | Air Operations Area |
| **ARFF** | Aircraft Rescue & Firefighting |
| **CCTV** | Closed Circuit Television |
| **CEO** | Chief Executive Officer |
| **CFR** | Code of Federal Regulations |
| **COO** | Chief Operating Officer |
| **DHS** | Department of Homeland Security |
| **DOT** | Department of Transportation |
| **FAA** | Federal Aviation Administration |
| **FBI** | Federal Bureau of Investigation |
| **FEMA** | Federal Emergency Management Agency |
| **FSD** | Federal Security Director |
| **GPS** | Global Positioning System |
| **IED** | Improvised Explosive Device |
| **IP** | Internet Protocol |
| **IT** | Information Technology |
| **MOU** | Memorandum of Understanding |
| **RFP** | Request for Proposals |
| **ROI** | Return on Investment |
| **SIDA** | Security Identification Display Area |
| **SOP** | Standard Operating Procedure |
| **SSI** | Sensitive Security Information |
| **TSA** | Transportation Security Administration |

# ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

| | |
|---|---|
| **AI** | Artificial Intelligence |
| **ASAC** | Aviation Security Advisory Committee |
| **CHRC** | Criminal History Record Check |
| **EAP** | Employee Assistance Program |
| **KCM** | Known Crew Member |
| **NOV** | Notice of Violation |
| **RFID** | Radio Frequency Identification |
| **SIEM** | Security Information and Event Management |
| **STA** | Security Threat Assessment |

# SECTION 1: WHAT IS AN INSIDER THREAT?

According to the TSA ASAC Insider Threat Subcommittee, insider threats are:

> Individuals with privileged access to sensitive areas and/or information, who intentionally or unwittingly misuse or allow others to misuse this access to exploit vulnerabilities in an effort to compromise security, facilitate criminal activity, terrorism, or other illicit actions which inflict harm to people, an organization, the air transportation system or national security.

An insider is someone who has, or once had, authorized access to information, facilities, networks, people, or resources. Whether intentionally or unintentionally, an insider can commit acts that violate law, policy, and procedures. These acts may result in harm from the loss or degradation of business operations, intellectual property, resources, or capabilities. An insider may also engage or facilitate external adversaries in destructive acts, such as physical destruction or harm to others in the workplace.

Insider threats to the aviation sector span all realms, including cybercrime, terrorism, and other criminal acts. Some of the more notable examples of aviation insider threats across the globe include smuggling of drugs or weapons, terrorism or sabotage, compromises in security, and destruction or theft of physical property.

Information in this guidebook aligns with these ASAC Focus Areas:

- Threat Detection, Assessment, and Response (Focus Area 1)
- Aviation Worker Vetting and Evaluation (Focus Area 2)
- Aviation Worker Screening and Access Control (Focus Area 3)
- Training and Engagement (Focus Area 4)
- Information Sharing (Focus Area 5)
- Governance and Internal Controls (Focus Area 6)

At airports, the pool of potential insider threat actors includes any individual who works at the airport in any capacity, including, but not limited to, management and administration, security and law enforcement, public safety, vending and concessions, and airlines/aircraft.

According to a recent study by the Ponemon Institute, the costs of insider threat incidents have increased 31% between 2018 and 2020, reaching an average of $11.5 million.[1] This research identifies insider threats from three major sources: employee or contractor negligence, criminal and malicious insiders, and credential thieves.

## 1.1 Risk Indicators, Behavior, and Motivation by Categories

The factors motivating someone to attack people and organizations are typically personal in nature (i.e., financial, political, and emotional). Because of this, threatening behavior can be easy to identify. The various threat types, their motivations, and potential behavioral indicators are outlined in Table 1.

**Table 1. Insider Threat Types, Motivations, and Indicators**

| Threat Type | Motivation | Indicators |
|---|---|---|
| Terrorist | Terrorists use insider access to facilitate or conduct acts to disrupt or coerce organizations for political reasons. | Terrorists may display nervous or secretive behavior, have suspicious foreign contacts, show interest in extreme causes, or have odd travel destinations. Other behaviors include threatening comments or threats of |

[1] Ponemon Institute, "2020 Cost of Insider Threats: Global Report," 2020.

| Threat Type | Motivation | Indicators |
|---|---|---|
| | | violence against the United States or individual citizens, sometimes through the internet and social media. Terrorists may also test an organization or facility by conducting probing activities, such as intentionally avoiding security cameras. They may show unusual interest in security matters outside the scope of their duties. |
| Spy | Spies use insider access to obtain sensitive or classified information for exploitation. | Spies may ask to work alone or on unsupervised shifts. They may avoid security cameras and show unusual interest in procedures, operations, and security matters outside the scope of their normal duties. When targeting specific individuals who have access to the aviation data they want, a spy may be overly eager or aggressive in attempts to develop friendships outside of their department or normal work area. They may attempt to copy private, internal information and their body language or movement may indicate they are taking photos discreetly. |
| Disgruntled Employee | Disgruntled employees often feel underappreciated or overlooked. They may have had a severe disagreement with their bosses, been subject to disciplinary action, or openly search for new employment while at work. They may have financial problems or other personal/home issues, and could be impacted by stress or other mental health issues. | Disgruntled employees may seek access to network servers outside of normal business hours. They may also request to work alone or on unsupervised shifts. They sometimes reveal dissatisfaction with rules, are frequently angry at coworkers or supervisors, and may express a desire for revenge. |
| Malicious Insider | Malicious insiders intend to cause harm or damage to their employment organizations or to an individual, for the purpose of personal gain or revenge. Motives can be political, economic, social, cultural, or personal. These insiders are aware that their access to materials, systems, networks, and infrastructure is valuable to terrorists and criminals. They may also be focused on advancing in an organization, or may already be in mid- or high-level positions with access to sensitive information but still feel they are undervalued. They are often motivated by money, title, and power. | Malicious insiders may receive an unusually high number of emails from external contacts, have frequent communications outside of the normal channels of an organization, and display a willingness to disobey rules to get ahead. |
| Compromised Conspirator | Compromised conspirators (including those who have been manipulated or coerced) may have financial or other problems that make them vulnerable to criminal or terrorist organizations. These organizations may attempt to address the individual's problems in exchange for leveraging their insider access. The insider may agree to sell or trade sensitive | Compromised conspirators may exhibit signs of financial instability (e.g., gambling activity or lavish lifestyle) outside of the work environment. They may have sudden, unexplained wealth, and try to conceal transfers of money or other financial resources into or out of the US. Displays of exuberant spending and luxurious travel may be posted on social media. They |

| Threat Type | Motivation | Indicators |
|---|---|---|
| | information, and thus become beholden to their benefactors for more. | sometimes have suspicious foreign contacts or travel. They may be involved in smuggling contraband or assist in providing unauthorized access to a restricted area. They may download or copy sensitive information or documents that are not relevant to their jobs. |
| Activist | Activists discover and copy private internal information about an organization, its operations, or its executives that can be used to damage reputations or cause embarrassment. | Activists may appear stressed, depressed, or energized by their beliefs. They seek access to sensitive information and often display dissatisfaction with rules. Any repeating minor rules violations may be indicative of greater problems. |
| Saboteur | Saboteurs seek to deliberately destroy or obstruct organizations and their operations, usually for some military or political advantage. They use their insider access to destroy equipment, materials, or information. | Saboteurs may have suspicious foreign contacts, travel to odd destinations, or engage in suspicious activity online and on social media. They may misuse credentials, avoid security cameras, and access network servers outside of normal business hours with increased downloading activity. |
| Thief | A thief uses insider access to steal information, intellectual property, or material items, usually for personal financial gain. Their activity can also include stealing passenger property. | Thieves may have a history of criminal activity or show unexplained sudden wealth. They may display nervous or secretive behavior, such as sweating, a lack of eye contact. They may also misuse credentials. |
| Negligent Employee | There are two types of negligent employees:<br>• Employees who are unaware of or misunderstand security procedures, leading to mistakes<br>• Employees who intentionally disregard security protocols for convenience or because they see them as unnecessary | It can be difficult to spot someone who makes an honest mistake unless an obvious security violation occurs. Those who intentionally disregard security protocols are generally sloppy, inattentive, and careless, and they can be too eager to please. They may openly share passwords, print sensitive information, allow unauthorized visitors, facilitate badge sharing, and “piggyback” at security gates and doors. |

Note that many behavioral indicators overlap among types of threats, which makes distinct categorization difficult. Regardless of the suspected threat type, all suspicious or unusual behavior should be reported immediately to law enforcement, airport security, or operations. Additionally, information should be relayed to available tip lines, the airport’s Insider Threat Risk Mitigation Hub (sometimes referred to as the Hub), or similar Insider Threat Working Group, if available. (Hubs are discussed in detail in Section 3.1 of this guidebook.)

# SECTION 2: DETECTION AND DETERRENCE

Detection and deterrence strategies are critical to the success of your Insider Threat Program. Integrating technology, people, and processes creates a framework of layers to combat insider threats. Airport operators should regularly evaluate their strategies, including associated financial considerations and the impact each has on risk.

## 2.1 Layers of Security

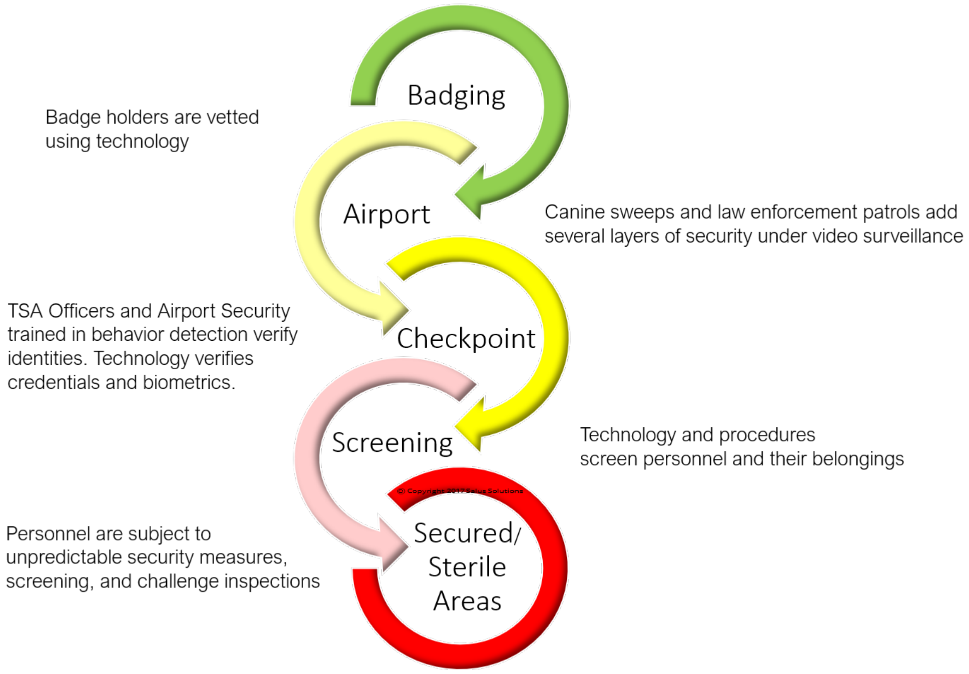
Information in this section aligns with these ASAC Focus Areas:

- Threat Detection, Assessment, and Response (Focus Area 1)
- Governance and Internal Controls (Focus Area 6)

Detection and deterrence are accomplished by layering security systems and practices, as shown in Figure 1, so that no one layer is a single point of failure. Layers may include physical barriers and operational processes, and are designed to stop a threat or reveal behaviors that may indicate a threat.

To be successful, layered security integrates people, technology, and processes throughout the entire airport environment to enhance awareness and timely reporting. Cooperation, education, training, and active participation are required to reduce and mitigate insider threats.

**Figure 1. Layers of Detection and Deterrence**



Badge holders are vetted using technology

Canine sweeps and law enforcement patrols add several layers of security under video surveillance

TSA Officers and Airport Security trained in behavior detection verify identities. Technology verifies credentials and biometrics.

Technology and procedures screen personnel and their belongings

Personnel are subject to unpredictable security measures, screening, and challenge inspections

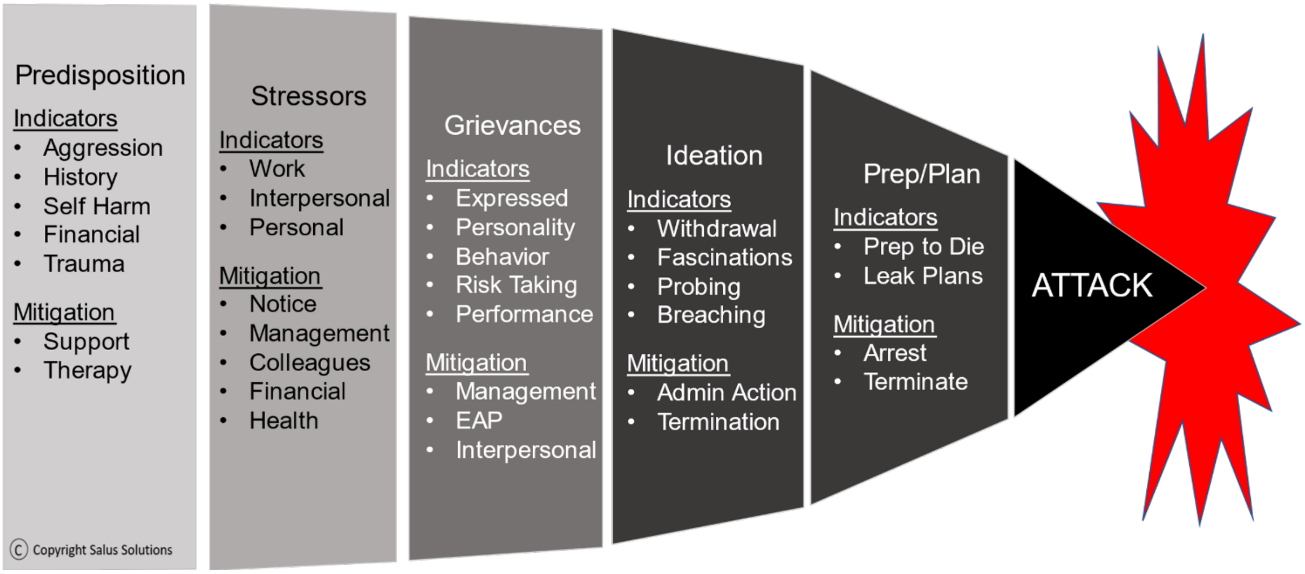
For example, the TSA has integrated layers of aviation security, some visible and many not visible. These layers include intelligence; other agencies; no-fly lists; crew vetting; canines; screening of people, baggage and cargo; inflight security measures; and passengers. Airport operators add even more layers to this model, with law enforcement and security personnel; employee vetting and credentialing; technology such as cameras, video analytics, and license plate readers; and physical security measures including controlled access points, fencing, gates, vehicle bollards, and explosives barriers.

## 2.2 Interdiction and Disruption

The development of an employee into an insider threat begins with a combination of individual factors and a precipitating event or accumulation of events. For example, an employee may be dealing with personal issues outside of work, such as financial troubles or divorce. That employee may also perceive an injustice has occurred in the workplace and become disgruntled. The perceived injustice alone, or in combination with the existing personal issues, could provide motivation for an insider attack.

Robust security programs that focus on identifying the early development phases of a threat can create opportunities to stop or disrupt it. Countermeasures such as those recommended in this guidebook can deter, detect, and mitigate an act through physical, procedural, and legal means. Figure 2 depicts indicators that, if recognized, provide an opportunity to mitigate a threat.

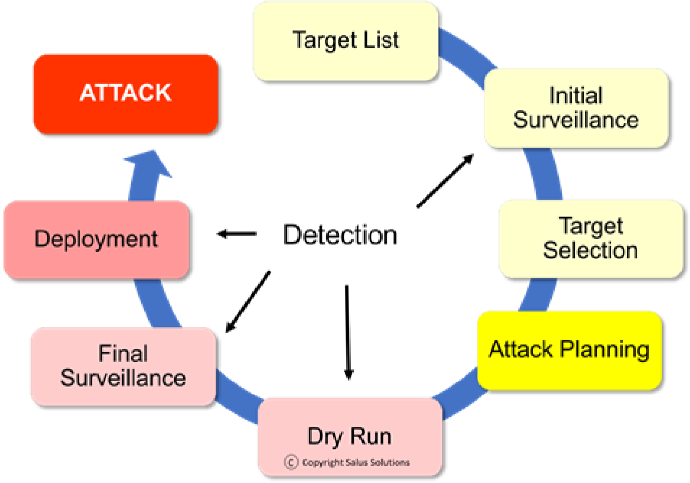
Figure 2. Perceived Workplace Injustice



Airports should be prepared to implement additional countermeasures when intelligence indicates the threat level has increased.

A threat actor's planning is essential to carrying out a successful attack. Understanding how an insider prepares for an attack helps the airport operator develop mitigation strategies and identify the most effective points to deter an attack. The Office of the Director of National Intelligence and other agencies use pre-attack planning cycles (similar to Figure 3) designed for detecting acts of terrorism; however, this cycle is also applicable to detecting insider threats.

Figure 3. Detection During Pre-Attack Cycle



## 2.3 Leveraging Technology

Technology provides critical tools for safeguarding access to physical and electronic assets. Control measures for physical assets span a wide range of technologies, such as cameras providing visual observation of people and cars, electronic door locks providing access control through keys or other tokens, radio frequency tagging to track equipment, and motion sensors providing proximity notification.

Protecting and monitoring electronic assets require numerous layers of security that include firewalls, protection from network intrusion, advanced threat protection, anti-malware software, and server-side access and activity monitoring. Stringent computer access rules are necessary and should include multi-factor authentication to deter breaches. Each of these measures typically provide, at a minimum, event logging that can be analyzed to monitor for threats. More advanced systems can also provide customized alerting that signals change in behavior, such as an employee logging in on their days off, or irregular patterns of use in days of the week or time of day.

### 2.3.1 CCTV and Video Analytics

Placing some cameras in plain sight, along with others in covert locations, can reduce the potential for an insider attack. Since insider threat actors often pay close attention to the location of cameras, those in plain sight can have a deterring effect. Concealed cameras provide an opportunity to observe an insider who may be conducting surveillance as part of their planning. Observing an individual conducting surveillance or attempting to identify the location of security cameras at prospective targets provides an opportunity to intervene and stop the threat. The observed behavior can also be used to build a more complete profile of the individual.

**It is important to place cameras where catering or other unobserved activities may occur**

When coupled with video analytic technology, cameras can be used to detect and alert on preconfigured event types. In an insider threat detection context, video analytics could be used, for example, to alert security to an individual in a defined location outside of normal work hours, or to someone who loiters in a sensitive area.

See Section 2.3.2 for information on camera-based facial recognition systems.

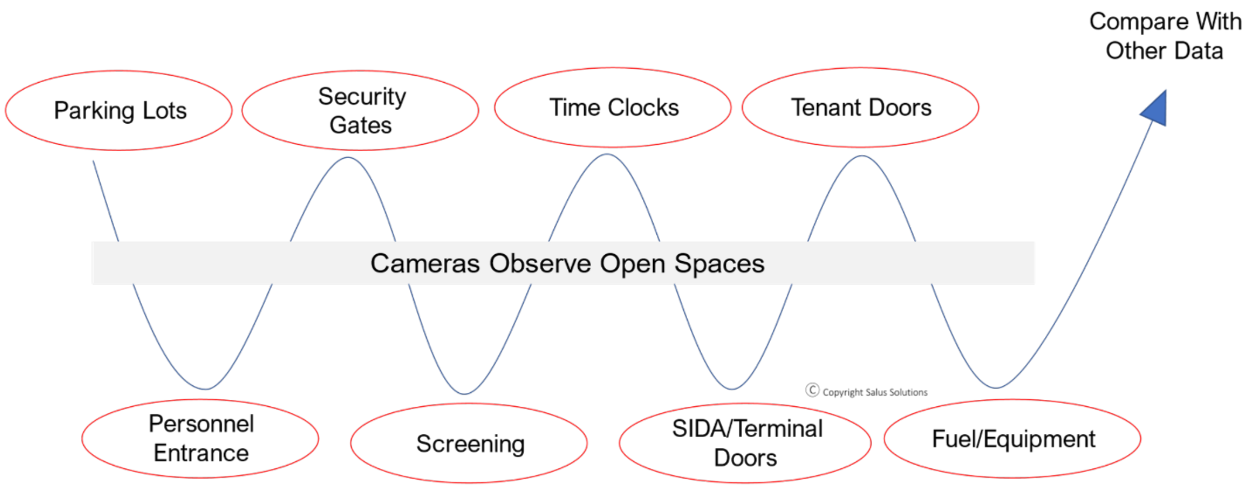
### 2.3.2 Biometrics

Contactless biometrics continue to improve in accuracy and their ability to provide efficient identification for access control. This technology can also be used with time clocks and equipment access, and to observe personnel through camera systems.

Camera-based biometrics can be used to identify faces and other identifying characteristics. Facial recognition can be used to compare the faces of people accessing secured areas to those of registered employees. If a face is not recognized, programming can require additional steps of authentication or lock a person out of the secure area, and the data can then be conveyed to security personnel. In addition, alerts can be generated when an individual is tracked to an area they would not normally visit.

Biometrics provide a layer of detection that can be integrated with other security data sources. Data from biometric systems can be analyzed to identify anomalies in patterns of behavior or map an employee's movement across the airport campus, as shown in Figure 4.

Figure 4. Biometric Layers of Detection and Deterrence



### 2.3.3 Limiting Remote Access to Computer Networks

Limiting remote access to an internal network is one of the most effective mitigation actions to protect data assets. An individual's need for remote access should be evaluated and granted only to those employees who need it to perform their duties. All devices accessing the internal network remotely require proper monitoring and must have approved security measures installed (firewall, malware protection, and access controls). The hard drives of the remote devices should be encrypted, and USB ports should be disabled. Remote access to the internal network should only be permitted through a Virtual Private Network (VPN) connection. Multi-factor authentication is recommended at each access point.

Organizational policies and controls for remote access should be established and well communicated. It may be necessary to disable access for one or more individuals with little advanced warning. For example, locking down an internal network or system in the event of a security breach or disabling access when an employee resigns or is terminated. While this task typically falls to the IT department, other teams must know who to contact at any time of day. Human resources, legal, and other management must closely coordinate to ensure remote access is disabled in a timely manner to thwart the potential for an insider threat.

### 2.3.4 Systems Integration and Analysis

The Internet of Things (IoT) comprises connected products like smartphones, smartwatches, radio and mesh networks (built-in repeating devices), access control systems, video surveillance systems, and vehicles and other equipment. These and other advances in technology are the reason for the exponential increase in data available to monitor.

Given the amount of data that could be collected from across the airport, reducing the human workload for examining this data is imperative. Systems integration and analysis tools, such as a Security Information and Event Management (SIEM) system, can integrate data from a wide range of monitoring systems into a single on-demand source to assess the airport's overall security posture and provide predictable security incident alerting. For example, license plate readers, access transactions, and personnel work schedules can be compared to identify whether employees are at the airport when they should not be, or are in locations they normally would not access. With the deployment of a modern integration technology backend, the collected information can be analyzed and shared with airport operations, law enforcement, and other key stakeholders.

Implementing a security incident integration and alerting system mitigates the potential to miss security incidents. However, these backend security alerting systems must be configured for the specific interfaces (device, appliance, sensor, etc.) that are being integrated. Ensuring the greatest return on investment for leveraging technology requires broad participation from organizational departments throughout the airport, including but not limited to Airport Operations, Security, and IT. As lessons are learned, the underlying rule sets must be adjusted to meet specific needs, which requires knowledge of the airport's environment and what the staff is already trained to watch.

Alternatively, an SIEM with artificial intelligence (AI) built in would have the ability to automatically analyze and learn from the data it ingests. AI can be used to detect the subtle anomalies that are characteristic of insider threats. The more data an AI system has, the faster it can learn, and the more accurate it becomes.

There are numerous systems on the market that are built by well-known, respectable software companies. Research summaries have been published by Gartner Incorporated that provide useful information for selecting SIEM systems, with or without AI capabilities.[2] Airport operators should consult with their security and information technology departments to evaluate emerging hardware and software technologies that could enhance the overall security posture of the airport. It is important to consider how these could be integrated with existing airport monitoring systems to detect potential insider threats.

## 2.4 Employee Vetting

Information in this section aligns with ASAC Focus Area 2, Aviation Worker Vetting and Evaluation

Employee vetting is a continuous, multi-layered process that includes initial vetting and credentialing and continues with periodic background checks.

49 CFR § 1542: Airport Security identifies the regulations for the airport credentialing process. Beyond the initial Criminal History Record Check (CHRC) and Security Threat Assessment (STA) required to receive a badge, airport operators must continue to monitor all employees through the renewal process (bi-annually at a minimum). In addition, the FBI's optional Rap Back service notifies participants when a change has occurred related to a badge holder's criminal activity.

**Management should approve the reactivation of any badge**

However, airport operators should also implement procedures to identify and document risk indicators (discussed in Section 1.1). Employee documentation includes information on credentialing, training, and disciplinary action. This information can be analyzed, and employees with a history of behavioral issues or poor work performance should be further monitored. Software is available that collects data on badge holders and assigns a risk rating to each individual. These services use behavioral science and machine learning to assess and prioritize which badge holders might be the highest risk.

[2] Gartner PeerInsights™, SIEM Reviews 2021: https://www.gartner.com/reviews/market/security-information-event-management

### 2.4.1 Badge Control

Airport operators are the credentialing authorities for airports. They can be affected by drastic and unexpected events. For example, during pandemics, natural disasters, or other unexpected events, large numbers of stakeholder employees may be faced with furloughs or layoffs eliminating their need for access to restricted areas. To compound matters, airport badging employees may need to work remotely due to social distancing requirements or environmental factors. As a result, the ability to suspend SIDA badges quickly and handle large volumes of work remotely creates unexpected challenges.

Employees with remote access pose an entirely new potential insider threat. Processes must be developed to track the behaviors and actions of remote employees. See section 2.3.3 for additional information on limiting remote access. Other questions to consider include: Do employees working remotely still need physical access to the airport? How long will it take to update thousands of badge holders in the system? Airport operators must identify solutions to reduce the insider threat risk in these situations.

One consideration is to implement an automatic temporary suspension of badges for the duration of furloughs. Another possibility is to require employers to take control of the SIDA badges and turn them in to the badging office for secure storage. A receipt should always be issued when a badge is returned to mitigate the vulnerability associated with returned badges that may be used inappropriately.

**Regularly reconcile SIDA badges with a system-generated, returned-badges report**

## 2.5 Personnel Screening

Information in this section aligns with ASAC Focus Area 3, Aviation Worker Screening and Access Control

Airports of any size can implement procedures for employee inspections. The method can be as simple as conducting random employee inspections using current operations, law enforcement or security staff, or it can be multifaceted, by installing employee-only screening checkpoints. Any of these changes require planning, but resources to support full employee screening require additional considerations and budgeting for equipment and staffing.

Conducting full employee screening prior to accessing restricted areas is effective for detecting and deterring threats, but it is costly to implement. It is also predictable, so potential threat actors may learn ways to work around the system. Repeated randomized inspections are not predictable and require fewer resources. Layering the two inspection approaches—full and random—in different areas of the airport, and at different times of day, creates uncertainty and increases deterrence.

Random inspections should be coordinated between multiple groups that conduct them, to ensure all locations are covered with adequate support. Unarmed security officers should always advise law enforcement prior to starting random checks at any location. Random inspections are more effective when conducted in numerous places at unpredictable times.

Random employee inspections should be highly visible and include physical/pat-down and personal property searches for fraudulent documents, badges, and contraband.

Airports need to constantly adjust practices based on what is occurring locally, regionally, and nationally. The focus of inspections is to mitigate, based on any current known possible threats and emerging threats. They can include drug smuggling, gun running, human trafficking or terrorist activities. Weekly meetings with security agencies (FBI, TSA, CIA, CPB, FAMS, etc.) ensures that emerging threats are identified and communicated.

**Provide a K-9 program to detect drug smuggling routes and tradecraft**

Additional information on this topic can be found in *PARAS 0019 Employee/Vendor Physical Inspection Program Guidance*.

## 2.6 Detection through Processes

Another layer of detection occurs in the processes by which activities are conducted. Whether in the separation of duties, permission for access to work areas, approvals for movement between duty stations, permission to change work schedules or staffing, or network separations, each step in a process is an opportunity to notice suspicious or undesired behavior.

The Insider Threat Working Group or Hub should work with all functional areas of airports and with all stakeholders to assess their processes, identify vulnerabilities, implement separation of duties, and to report activities. (Hubs are discussed in detail in Section 3.1.)

## 2.7 Physical Security

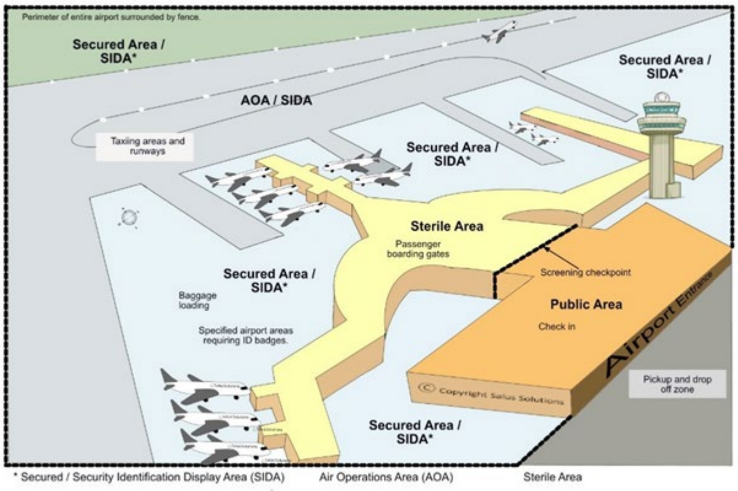
Physical security (doors, gates, walls, fencing, etc.) allows for separation based on the security level and specific duties of an individual's job functions. Airport operators can develop a series of access levels that correlate with their organizational structure.

### 2.7.1 Reducing and Controlling Access Points

Reducing the number of access points to the sterile and SIDA areas and along the airport perimeter provides more effective control of those areas and requires fewer security personnel to maintain operations. These security personnel can then be used to increase random inspections and patrols within the secured area.

Where possible, create a single "public to Sterile" access point at each terminal. In addition to private contract security providers, the TSA may be available to provide staff to perform inspections during select time periods. Full employee inspection programs are an effective means to reduce contraband entering the sterile area. Additionally, a single access portal provides a cost-effective way to install high-definition video that is suitable for use with analytics and facial recognition.

Figure 5. Airport Security Areas



Gate access points should be reviewed periodically to determine their continued need. If possible, create one staffed access point, where vehicle inspection and verification of employee credentials are conducted, and any escort activity is documented.

All changes should be communicated well in advance through multiple channels and various media. Since removing access points may cause delays in employee access, airports can work with affected stakeholders to develop a gradual reduction schedule to allow employees to adjust. Staggering shift start and end times can help to reduce lines at screening locations. When considering closures, it is essential to ensure that appropriate emergency ingress and egress is maintained.

Access points can be further controlled by eliminating or reducing the use of physical keys by implementing credentialed electronic access. These systems can offer touchless access, and they are faster to reset than traditional keys when one is lost.

If keyed access is essential, ensure keys are stored in a secured location, require management authorization to determine who can access keys, limit the number of keys personnel can access, and create a key custody/accountability system for signing keys in and out. Key safes can be used to allow emergency responders access when needed. Another option is an electronic key management system, which allows for keys to be programmed, tracked, and audited. These systems can be supplemented with customized electronic key cabinets that create an entry log and can send alerts if a key is removed by an unauthorized person.

### 2.7.2 Personal Location Systems

Personal location systems work by tracking personnel and assets on airport property. Real-time employee tracking systems use GPS, active radio frequency identification (RFID) and Bluetooth Low Energy beacon technology to track badges distributed to personnel. Real-time locating system receivers are installed throughout the work area to track the badges. These receivers are usually placed in strategic spots, such as entryways, exits, high-risk areas, hallways, breakrooms, outside areas, and parking lots.

Geofences can also be used to locate personnel on airport property. This technology uses GPS and RFID to create lines of demarcation that send alerts when personnel cross that line. They can use tracking software, allowing for total control and visibility of the entire tracking system, set up automated alerts, add and edit badge information, define unwanted activities, implement badge transaction analytics, supplement access control systems, and create reports.

# SECTION 3: INFORMATION SHARING AND COLLABORATION

Information in this section aligns with these ASAC Focus Areas:

- Threat Detection, Assessment, and Response (Focus Area 1)
- Information Sharing (Focus Area 5)

Information sharing and collaboration are critical to a successful insider threat program. Countering insider threats requires collaboration throughout the entire aviation ecosystem. This ecosystem is extremely complex, and interdependent relationships between governmental and public agencies, airlines, third-party providers, the public, media, and supply chains necessitates the need for collaboration within layered security systems in place today.

While the benefits of stakeholder engagement vary based on the circumstances of each airport, in general, it does contribute to greater understanding, compliance, information and data exchanges, as well as collaboration between all relevant parties. As new processes and technologies are implemented in and around airports, all key stakeholders hold a “piece of the puzzle.” As everyone works together, the puzzle is put together and vulnerabilities are identified allowing mitigation measures to be implemented.

Whether insider threat incidents are caused accidentally or maliciously, they cannot be mitigated with technology alone. Airports should develop an insider threat management program that combines people, processes, and technology to identify and prevent incidents. The program should comprise several components:

- Information sharing
- Interagency collaboration
- Incident analysis
- Communications
- Memorandums of understanding

## 3.1 Insider Threat Working Group or Hub

Insider threat experts recommend developing an Insider Threat Working Group or Hub to bring together agencies and stakeholders that have a role in combatting insider threats. These groups are useful for creating relationships, sharing information, and developing strategies for facilitating recovery plans. Whether formal or informal, they are the starting point for multiagency cooperation, collaboration, and information sharing.

### An Effective Insider Threat Mitigation Program

✓ **Identifies and focuses on those critical assets, data, and services** that the organization defines as valuable

✓ **Monitors behavior** to detect and identify trusted insiders who breach the organization’s trust

✓ **Assesses threats** to determine the individual level of risk of identified persons of concern

✓ **Manages the entire range of insider threats** , including implementing strategies focused on the person of concern, potential  ctims, and/or parts of the organization vulnerable to or targeted by an insider threat

✓ **Engages individual insiders** who are potentially on the path to a hostile, negligent, or damaging act to deter, detect, and mitigate

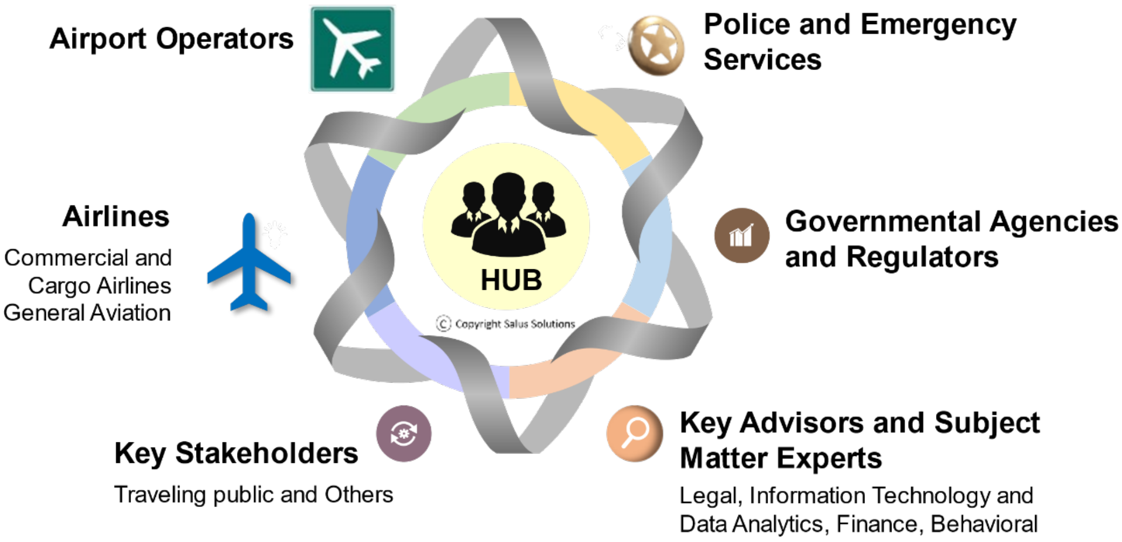
Though law enforcement personnel want to be involved when action or investigation is warranted, they may not want to lead or facilitate the group. With a vetting program, physical security, and access control system responsibilities and authority, airport operators are in the best metaleadership position to organize, facilitate, and lead the group and the exchange of information. Even if an airport operator does not want to lead the group, they can serve as great facilitators to bring the collaborative parties together and help define the group's mission.

The success of an Insider Threat Working Group will depend on the commitment and participation of all members and stakeholders. At a minimum, the  Airport Security Director, the FSD, Deputy Security Director, Assistant FSD – Law Enforcement (AFSD-LE), and senior manager should be members of the working group.

The Hub model involves a community-wide approach with broad stakeholder participation in detecting, deterring, and mitigating the risk of insider threats. It can also include a center for best practices. Formal partnerships streamline processes and leverage relationships to mitigate risk. It is extremely difficult for a single entity to detect or counter insider threats. Aviation security agencies and stakeholders may have differing perspectives, and each may own data sets that are useful in detecting insider threats.

**Figure 6. Insider Threat Hub Stakeholders**

**Collaboration is the key to success!**


Airport Operators
Police and Emergency Services
Airlines
Commercial and Cargo Airlines General Aviation
HUB
© Copyright Salus Solutions
Governmental Agencies and Regulators
Key Stakeholders
Traveling public and Others
Key Advisors and Subject Matter Experts
Legal, Information Technology and Data Analytics, Finance, Behavioral

The National Insider Threat Task Force (NITTF) "2017 Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards" recommends a four-step process for implementing a Hub:

1. Identify agency components that are likely to possess information of interest in insider threats
2. Collaborate with each component to determine information that would be useful in detecting behavioral anomalies
3. Determine how relevant data can flow efficiently to the Hub
4. Determine how to staff the Hub

Best practices for Hubs suggest each member agency or stakeholder designate a senior official to have responsibility for the agency's participation. The benefit to the Hub model is its holistic approach to identifying potential insider threats, and each representative brings different resources to the group. Putting all the pieces together provides a better picture of the threats and risks as well as how to mitigate them.

For more information and tools, see the Insider Threat Working Group or Hub Planning Checklist and List of Potential Stakeholders in the appendix of this guidebook.

## 3.2 Data Sharing and Data-Driven Decision Making

When data is shared by numerous agencies and stakeholders, finding ways to optimize data-driven decision making can be a daunting task. There are many technology platforms and databases to consider, and those systems are owned and operated independently. One of the greatest challenges for airports is analyzing the vast amount of available data to detect subtle behavioral anomalies and alert authorities, or the Hub, for possible investigation. Establishing an insider-threat case-management system facilitates tracking and monitoring for investigations. These investigations can also be managed and coordinated through Hub agencies.

**Establish a repository for all completed Insider Threat investigations**

For example, an airport operator can provide SIDA data to airlines for their employees through regular batch downloads. The airline can then compare this data with the airline employee work schedules. Using business rules and algorithms, airline personnel could then be alerted when an anomaly is detected, allowing the airline to investigate the incident and determine whether an issue exists.

The NITTF 2017 Insider Threat Guide, Section VI, Information Integration, Analysis, and Response addresses how to build and maintain analytic and response capabilities. Several best practices are identified, including creating an insider threat Hub, centralizing capabilities, deconfliction, sharing agreements, quality reviews, behavioral science, and analytics.

## 3.3 Information Sharing

The regular exchange of information is critical to stopping insider threats. Information sharing allows one entity to learn from the successes and failures of another. Exchange of information that meets privacy mandates and guidelines should foster open lines of communications during routine and crisis situations, and for efficiency and operational security between stakeholders and identified threat data.

Some airports have daily meetings of 15–30 minutes to discuss events and exchange information. Other airports have monthly or quarterly meetings to exchange information and focus on trends and issues affecting their insider threat risks. Best practices recommend that information sharing be managed by the security director, law enforcement insider threat leader, or an insider threat coordinator.

When data requests are received from agencies and stakeholders, airport operators can require the requesting agency to identify the threat and reason for the inquiry. Two-way exchange of information helps alert other stakeholders to the need for additional investigation, and helps build a more complete understanding of a potential threat.

An insider threat program may receive information from data access patterns, network user activity, or employee reports. This information can then be analyzed to obtain the overall level of a possible threat, and appropriate action can be taken based on unwanted behavior as defined by the airport. This response may include a referral to human resources, an employee assistance program, law enforcement, or the FBI. After a referral is made, the insider threat team should continue to monitor the outcome and use the event for training. Providing feedback and establishing a dialog between internal and external entities provide a forum to update and deconflict with stakeholders. While it is difficult for airport operators to be fully aware of disciplinary issues with stakeholders, the airport operator may consider encouraging stakeholders to share that information to evaluate risk.

Since airport operators also perform regulatory functions, they should create a collaborative strategy for sharing information with airlines, vendors, and other stakeholders. Stakeholders must be allowed to disclose sensitive information to members of the Hub without fear of regulatory reprisal. Airport operators should also train and encourage airport personnel to report their own live events and behaviors that may attract concern from others. This practice normalizes the reporting of concerns, and reduces the time required to investigate reports.

Tips for information sharing include:

- Identify working group or Hub members
- Generate buy-in and understanding at the senior leadership level for all agencies and stakeholders participating
- Consider agreements with key organizations through memorandums of understanding or agreement
- Evaluate data exchange possibilities and joint analytics
- Identify how investigations will be coordinated
- Develop awareness and training programs
- Incorporate all partners into training and exercises
- Ensure each member knows what information can and cannot be shared in compliance with applicable laws

Information sharing strategies should also be included in training and exercises (see Section 4.1).

### 3.3.1 Law Enforcement

Law enforcement agencies play a vital role in the working group and Hub. They have unique intelligence capabilities and an infrastructure that can support investigative activity and response. Airport operators should meet with appropriate law enforcement agencies to determine the possibilities for exchanging information for criminal investigations, incident response, intelligence sharing, and insider threat cases. Depending on the size of an airport, many law enforcement agencies could have jurisdiction at and immediately adjacent to the airport.

One best practice is for the airport's security coordinator or airport police to facilitate monthly or quarterly meetings for the exchange of law enforcement intelligence. This brings together representatives from all law enforcement agencies to discuss cases, intelligence, and advancements in technology. Generally, only law enforcement officials should attend this meeting.

Another recommended practice is to create an emerging threat group. This group consists of key federal, state, and local law enforcement agencies operating within the airport community. As an emerging threat or situation is identified, electronic communication can be sent rapidly ensuring all members have immediate awareness of a situation.

### 3.3.2 Air Carriers

Many air carriers have established insider threat programs in their own companies. Their participation in a working group or Hub provides timely and valuable information, including employee information, work schedules, flight schedules, passenger data, equipment information, and holiday or surge schedules can help provide a broad and clear picture of what employees are doing versus what they should be doing. Any anomalies or discrepancies in the data should trigger a follow-up to determine if there are any insider threat risks.

Airline and airport IT systems may not automatically exchange information. Airport operators are encouraged to meet with each airline and determine how their programs can be integrated for a coordinated response. In many cases, an airline's insider threat representative may be at its corporate headquarters or regionally based. Contact with the air carrier station manager is a good first step to determine the best representative for the airport.

### 3.3.3 Other Stakeholders

All airport stakeholders need to feel a part of the insider threat community. It is everyone's responsibility. Having a "see something, say something" policy with the appropriate training will enhance information sharing throughout an airport. Additionally, it helps to create a culture of commitment to not allow threats to develop in one's own community, where all parties understand their role in preventing threat actions.

One of the biggest challenges for airport operators, and other regulators, is working with stakeholders to promote a collaborative security culture while maintaining regulatory oversight. This challenge presents a delicate balance and working through violations can be a sensitive issue. With the implementation of a Hub, regulators and stakeholders must agree on how infractions are dealt with by the Hub. Trust must be established for effective collaboration. Airlines must be able to discuss behavioral indicators and how threat actors can exploit their access to the aviation system without fear of regulatory actions. A best practice that airport operator's may want to consider is identifying those employees using their airport access privileges when they are not working or on official business. This may require collaboration between airlines, vendors, and regulatory officials to identify situations requiring additional investigation or follow-up.

The airport should develop a matrix for stakeholder notifications to manage notification priorities based on roles and responsibilities.

### 3.3.4 Collaboration and Data Exchange Case Study

A great example of information sharing between stakeholders is the Known Crewmember® program (KCM). KCM is a risk-based system that enables TSA personnel to electronically verify the identity and employment status of active flight crewmembers. The program is sponsored by the Air Line Pilots Association and Airlines for America. KCM integrates personnel data from participating airlines into a single system, allowing TSA to verify flight crew members who are enrolled in the system.

In response to COVID-19, KCM posted the following bulletin on their website:

> Due to the unprecedented impacts of COVID-19 on commercial airline service, many airline employees including crewmembers have taken an extended voluntary leave of absence. The Known Crewmember Program® is a risk-based system that enables TSA security officers to positively verify the identity and employment status of active pilot and flight attendant crewmembers (i.e., flying the line). Crewmembers on short term disability, long term disability, Family Medical Leave Act, military deployment, voluntary leave of absence, furlough, suspension, termination, retirement, or other leave of absence must be suspended or removed from the KCM® system. Upon returning to work, it is recommended that the crewmember contact their airline management or crew records department to see if your KCM® file has been reactivated. This will ensure your ability to use the KCM® system again.

This is a great example of how shared information can reduce risks associated with insider threats. Airport operators are encouraged to work with their stakeholders to discuss innovative solutions that not only mitigate insider threat risks but also increase efficiencies and cost savings.

## 3.4 Cost Analysis

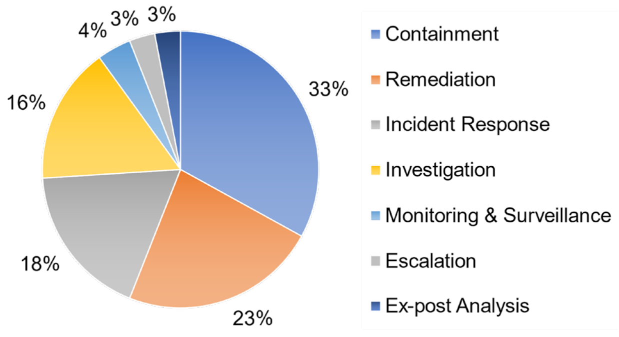
To assess the impact of insider threat activities, and the benefits of instituting an Insider Threat Working Group, it is important to understand  the financial impact and cost associated with preventing and mitigating these threats. Below is a summary of Ponemon Institute's 2020 Cost of Insider Threats Global Report, which describes the impact of insider threat mitigation on an organization.

- Theft or loss of mission critical data or intellectual property
- Impact of downtime on organizational productivity
- Damages to equipment and other assets
- Cost to detect and remediate systems and core business processes
- Legal and regulatory impact, including defense cost
- Lost confidence and trust among key stakeholders
- Diminishment of marketplace brand and reputation

The study also defined seven core process-related activities or internal cost activity centers:

- **Monitoring and Surveillance** – Activities that enable an organization to reasonably detect and possibly deter insider incidents. This includes overhead costs of technologies that enhance early detection or mitigation.
- **Investigation** – Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents.
- **Escalation** – Activities taken to raise awareness about actual incidents among key stakeholders in the company, including the steps taken to organize an initial management response.
- **Incident Response** – Activities relating to the formation and engagement of the incident response team, including the steps taken to formulate a final management response.
- **Containment** – Activities that focus on stopping or lessening the severity of insider incidents. These include shutting down vulnerable applications and endpoints.
- **Ex-post Response** – Activities to help the organization minimize potential future insider-related incidents. These also include steps to communicate with key stakeholders, both within and outside the company, and the preparation of recommendations to minimize potential harm.
- **Remediation** – Activities associated with repairing and remediating the organization's systems and core business processes. These include restoring damaged information assets and IT infrastructure.

**Figure 7. Percentage of Insider Threat Incident Costs**



Researchers found that companies spend an average of $645,000 on each incident, with containment and remediation being the most expensive activity centers, while ex-post response and escalation are the least expensive. Researchers also found that companies' costs for investigation and escalation are increasing. Regardless of the activity center, costs are being driven by added personnel and technology to resolve insider incidents, at a rate of $46 dollars out of every $100 dollars spent.

According to the study, the worldwide annual cost of insider threats has risen 31% to an average of $11.45 million per company. Companies in North America are exceeding the global average experiencing the highest total cost of $13.3 million annually, as compared to the Middle East, Europe, and Asia-Pacific regions in the study.

To be ready for these increasing trends, airports' Insider Threat Working Groups or Hubs should establish appropriate budgets to mitigate the risks associated with insider threats. The hubs should also understand that the faster a threat is contained, the lower the cost. Many companies are therefore deploying cost-saving tools and activities such as user behavior analytics, privileged access management, user training and awareness, security incident and event management, threat intelligence sharing, strict third-party vetting procedures, incident response management, employee monitoring and surveillance, network traffic intelligence, and data loss prevention.

# SECTION 4: CREATING A SECURITY-MINDED CULTURE

Information in this section aligns with ASAC Focus Area 4, Training and Engagement

A strong security culture starts with clear leadership that has the authority, resources, and training to implement policies, procedures, and training programs. The overall objective is to identify suspicious actions within the organization or the airport, and to determine what actions to take upon identifying a threat.

Strong executive leadership is critical for developing a security-minded culture. Senior leaders must convey to their employees and partners the importance of a strong insider threat program. Best practices include having a senior executive accountable for meeting goals and implementation strategies. Such leadership informs and sets an example for employees. A weak security culture, with unclear leadership structures, makes it less likely that individuals will report suspicious activities.

Security programs need to evolve and change as the threat landscape changes. In addition, these changes must be noticeably incorporated into procedures and training. Such transparency breeds confidence that the reporting process provides accurate information, leading to quick responses.

## 4.1 Training and Awareness Strategies

Insider incidents at airports can compromise national security, cause loss of life, compromise classified information, and lead to lost revenue related to theft of secrets, fraud, sabotage, damage to an organization’s reputation, acts of workplace violence, and more. A critical component of the defense against an insider threat is a well-informed and properly trained workforce, to serve as human “sensors” and alert authorities about unusual behavior.

### 4.1.1 Training Topics

Leadership should train the workforce to recognize threats posed by insiders, as well as their responsibilities for reporting suspicious behavior. Recommended insider threat program training, at a minimum, includes the following topics:

Take violations and turn them into training topics

- Importance of insider threat awareness
- Purpose of an insider threat program
- Purpose and function of the airport’s Insider Threat Working Group
- Behavior indicators and motivation factors
- Recognizing and reporting indicators of insider threat
- Security and counterintelligence
- Avoiding a ‘witch hunt’ atmosphere
- Methods for reporting (tip line, email, text, person to person, tip box, smartphone apps)
- Reporting forms
- Aspects of a good report (clarity, context, credibility)
- Impact and reporting of positive and negative life events
- Risk indicators
- Biases
- Gaps in information

All employees should be trained to recognize direct and indirect threats. Direct indicators include downloading data to external drives, accessing sensitive information not relevant to job duties, or attempting to enter locations without authorization. Indirect indicators include patterns of behavior that require analysis to reveal suspicious motives. Examples include sudden extreme negativity, expressing a desire to resign, and demonstrating connections to high-risk personnel or outside parties. Employees should have an easy way to report any of these types of suspicious behavior. See Section 4.2, and Appendix A for an observed behavior report form template. Training should emphasize the importance of reporting the concern rather than being correct in one's observations.

### 4.1.2 Training Frequency and Delivery Methods

Airport operators should require insider threat training to be completed as part of the credentialing process. If this is not possible, a best practice is for employees to complete this training within 30 days of receiving their badge.

Recurrent training should occur with every badge renewal, or at most every two years. Each airport has different needs, depending on size and use. The type of training provided helps to determine frequency. For example, in-person classroom training, which is the costliest practice, may occur annually or biannually, while computer-based training, which individuals can complete anywhere and anytime, can be conducted more often. Ten-minute rehearsal of concept talks are very cost effective and can be completed weekly or monthly depending on the department and the need.

Because individuals learn differently, it is most effective for insider threat training to be offered in a variety of formats. The most effective method is in a classroom setting, which facilitates discussion of actual examples (case studies), of possible motivations behind threat actions, and of how an organization can intervene to help potential threat actors before they act. An interactive webinar or computer-based training can also be effective.

Support and reinforce training with an insider threat SOP or manual, quick reference cards, posters, and flyers, internal emails, videos, all-hands meetings, etc. Provide these materials and information to all levels of the organization to raise awareness about insider threats and encourage employees to be involved in the airport's program. Host an Insider Awareness Day with a guest speaker, live forum, or live streaming webinar. All training materials should be readily available to employees.

### 4.1.3 Assessing the Training Program

Determining the effectiveness of training programs is essential for continuous improvement. An easy way to evaluate training is to ask participants to complete questionnaires before and after the training. Programs can also be evaluated by testing, surveys, data calls, and student feedback.

Key performance indicators should be developed to compare post-training data to baseline metrics (e.g., number of threats mitigated, reports filed, reduction in violations, etc.) This enables the airport to determine the impacts of the training on their insider threat vulnerability, and which aspects of the training may require more emphasis or changes to produce desired outcomes. Based on pre-training surveys and post-training evaluations, identify best practices, lessons learned, and new ideas for future programs.

A process should be established for maintaining records, certificates of completion, or other documentation on all those who have completed initial and annual training, including individuals who started the credentialing process but were not cleared to receive a badge.

## 4.2 Reporting Mechanisms

A successful insider threat program requires multiple methods for reporting suspicious behavior. These methods may include person-to-person reports, phone numbers for anonymous tips, text messaging, email, mobile phone applications, and handwritten notes in a secure box. Reports are then evaluated by the airport's Insider Threat Working Group for further action.

The mechanisms by which reports are made are important. Airports can use an evidence-based system to accurately report information and to judge the credibility of reports. Without a proper framework, important information can be misreported, misinterpreted, or overlooked. An evidence-based framework also helps to overcome bias, the misreading of situational influences, and an over reliance on risk indicators as a reason to report suspicious behavior.

### 4.2.1 Clarity, Context, and Credibility

Reporting effectiveness is measured by the clarity, context, and credibility of the reports.

**Clarity** stems from reporting without personal judgement. This allows for more than one explanation or conclusion to be drawn from the report. Reports that include interpretations, impressions, or conclusions may lack the necessary information to present pure observations or situational facts.

Here is an example of a report containing only interpretation, impression, or conclusion:

> My new co-worker is unreliable and acts strangely, and I think he is involved in something illegal.

Here is an example of an evidence-based report that brings clarity to information:

> On Monday, my new co-worker clocked-in at 8 a.m., but I did not see him until two hours later. The next day I noticed that same co-worker lingering around the fence. He bent down, picked something up, placed it in a box, and put it in the locked storage room. Then on Wednesday, while driving to work I noticed my co-worker was talking to some strangers at a gas station. They both had their car doors open.

**Context** surrounding observed behavior is important to creating an accurate assessment. This includes detailed information that describes how the reporter happened upon the observed behavior and what exactly he or she saw. To avoid mistakes in assessing a potential risk, reports should provide alternative explanations for an observed behavior, how the reporter knows the information, exactly what they know, and from whom, whether by telephone, person-to-person conversation, or visual observation. And what time of day the observation occurred, the location, who was there, the situation, events, and actions during the observed behavior.

Here is an example of a report with proper context:

> On Monday, my new co-worker clocked into his shift around 8:00 a.m. Around 10:00 a.m., I observed him walking from the direction of the human resources office with a large manila envelope in his hand. He also had a smile on his face. The next morning around 9:30 a.m., I observed my co-worker near the fence line. He bent down and put something in a box, and then placed it in the locked storage room. I thought it was odd because the box had a few holes in it, and the storage room is not normally used. Then on Wednesday, at 7:15 a.m., I observed my co-worker at a gas station near the airport. His car, a small black sedan, was parked on the side of the gas station. Parked next to him was a silver minivan. Talking to my co-worker was an adult female, an adult male, and two children. It's possible that the envelope contained a list of items to be stolen from the airport and sold on the street. I guess it's also possible the envelope and the box had nothing to do with the meeting at the gas station.

**Credibility** of the person making the report is an important factor when assessing the information. Not every report is clear, has contextual information, nor objectivity. The relationship of the reporter to the observed behavior is an important component to the assessment. Questions for consideration are:

- Is this a direct observation or an assumption?
- Are there conflicts between the reporter and the subject?
- Do the reporter and the subject normally have much contact with each other?
- Why is the reporter making this report at this time?
- Did the observed behavior occur in a usual mode of communication?
- Does the reporter have influence over the subject's performance evaluations?
- Does the reporter generally have exposure to this information?
- How knowledgeable is the reporter of normal airport operations and activities?

Here is an example of credibility of the reporter:

> The reporter worked in the same position much longer than the subject and had recently applied for the same internal promotion opportunity as the subject. The reporter's wife left him and moved the kids out of town. The reporter now demonstrates a negative attitude towards women and coworkers with children. This information demonstrates the reporter may have other reasons for filing the report, which might make the reporter less credible.

Here is the analysis of this scenario by the airport's Insider Threat Working Group:

> With information regarding the clarity, context, and credibility of the reporter, and following preparation of the report, the airport's Insider Threat Working Group was able to determine the co-worker was called to human resources on Monday morning to receive a promotion. The suspicious item picked up near the fence was a kitten, and by calling the phone number on the collar, the subject was able to return the kitten to its family the next morning.
>
> It is important to note that if the co-worker had self-reported that he found the kitten and was returning it to the family, formally or informally, this matter would have been easier to resolve.

### 4.2.2 Developing Reporting Mechanisms

Clear reporting mechanisms can help the airport collect useful information and avoid overlooking any suspicious behavior or false accusations from misinterpreted observations. A successful framework for reporting mechanisms not only educates airport personnel about risk indicators, but also build awareness of how social situations and biases influence what we see and what we give attention to. Several considerations are necessary for effective reporting mechanisms:

Create a **standard form** to:

- Document what behavior is observed or verbalized
- Helps reduce biases or omissions that can occur when memory is relied upon
- Improve timeliness, transparency, standardization, analysis, and accountability

Provide an **example** of a good report. A good report:

- Provides clarity, context, and addresses credibility of the reporter
- Provides alternative examples for a subject's behavior
- Shows the relationship of the reporter to the observed person, describing it in terms of frequency, intensity, and duration

- Shows repetition in dissimilar situations
- Comes from sources who do not have a stake in the outcome
- Is documented according to time, place, and situation

Require **context** be accounted for:

- Caution that not everything is relevant
- Require time, place, setting, numbers of people, rank and position of individuals present at the time of the observation
- Require a statement that the reporter either is or is not sure how the statements or behaviors came about

A sample report form is provided in Appendix B of this guidebook.

Require **training** for all personnel. A critical component in reporting is to distinguish simple, objective information from subjective information. Integrate insider threat training into the airport's training program and focus on the list of topics and content found in Section 4.1.1 Training Topics and Content.

Require information that assists in **analysis** of a reporter's credibility and potential motivations for reporting. Require information about the reporter, the quality, the duration, and the level of contact with the subject. Opinions about co-workers are unavoidable and will often introduce bias in reporting. Managers have perceptions about their subordinates, and subordinates may distrust or even fear their managers. A report should not be ignored because of the reporter's credibility. Understanding the relationships and other predispositions of the reporter will assist in the analysis of the credibility of a report.

Prepare reports for **evaluation**. Before a report is ready for evaluation by the Insider Threat Working Group, a member of the group must prepare it for presentation to the whole group. Presentations of reports assist in identifying gaps in the information and indicate what information is needed to verify statements. This involves analyzing the report for clarity, context, credibility and identifying any statements of bias or opinion. It is suggested that the preparation also require alternative explanations of behavior to be generated, about why the behavior may not be a threat.

An accurate assessment of a subject's behavior requires looking at the totality of events to better understand the individual's behavior and their risk potential. Social media and other open-source material can provide information that is valuable in evaluating an employee's potential as an insider threat.

Care must be taken not to embarrass or show disregard for employees who make incorrect, but good faith, notifications of security violations or suspicious behavior. The analysis of and lessons learned from these incidents feed information back to the program for continuous development and improvement.

### 4.2.3 Privacy and Civil Liberties

When considering an airport's reporting mechanisms, three main areas of employee protection to consider are privacy, civil liberties, and whistleblower protection. The Privacy Act and Whistleblower Protection Act are federal laws, and civil liberties are broadly protected by the U.S. Constitution. Insider threat programs are designed to manage risks associated with malicious or unwitting insiders, while protecting privacy and civil liberties. Emphasize to employees the importance of early intervention and transparency to minimize misconceptions of over intrusiveness. Also emphasize how insider threat reporting procedures are designed to protect the privacy and civil rights of the workforce. Airport operators should seek legal review of insider threat policies, procedures, and forms prior to implementing them.

Educating the entire airport community on the importance of an insider threat program is more important than just having a program in place and appearing to comply. Employees and people familiar with the airport environment are a great asset for accurate and timely monitoring. Avoid a hostile atmosphere with a well-designed, fair, and open reporting process and proper training. This education manages employees' expectation of privacy and reduces risk of retaliation against the organization.

# SECTION 5: WORK ENVIRONMENT AND EMPLOYEE ASSISTANCE

Good workplace mental health and wellness practices help keep stress levels in check and provide a supportive environment. Empowerment, engagement, growth, satisfaction, and trust programs help maintain a positive work environment. These practices also guard against some motivators and opportunities that drive insiders to act negatively.

## 5.1 Engagement Programs

Employee engagement is an indicator of how invested an individual feels in their organization's mission and values. An engaged employee feels involved and respected in the workplace, and as a result is more likely to stay with the organization longer, work harder and more cooperatively, share knowledge, and solve problems more effectively. A disengaged employee, on the other hand, has a more negative view of their workplace, and is more likely to perform poorly and become disgruntled. It is therefore important to assess and manage employee engagement levels in order to minimize the potential for developing insider threats, while maximizing employees' desire to remain vigilant and protect the airport from bad actors.

Engagement programs support motivation, attitude, initiative, satisfaction, and overall company performance, and aim to reduce turnover. These programs should be specifically tailored to the organization to be most effective. For example, allowing employees to make independent choices leads to innovation and increases empowerment. This practice might induce employees to take a more active role in observational security.

Recognizing quality performance encourages employees to give greater attention to detail, job proficiency, and customer interaction. Examples of high-quality employees include officers with the most positive customer feedback and supervisors and managers with the lowest safety accident rates. Greater quality can also reduce the costs of litigation, insurance, and lost productivity. Training and education facilitate developing these qualities in the workforce.

The constantly evolving work environment requires innovation and flexibility. Encouraging initiative empowers employees and bolsters creative thinking. Airport operators may consider recognizing the contributions of employees or teams that successfully develop ideas or solve problems outside of their respective job functions. Providing employees with opportunities for growth can help increase job satisfaction.

Seeing improvements in their self-directed, team-oriented effort is also motivating and can improve employee retention.

Trust improves with fair and transparent employee review methods, procedural fairness, and managers who are authentic and engaged with employees on a human level.

### 5.1.1 Reward and Recognition Programs

A circular relationship exists between rewards and recognition, job satisfaction, and job motivation for workers. Rewarding and recognizing workers has an important role in engaging employees in an organization's culture. Airport operators wanting to promote a security-minded culture can consider implementing some form of recognition and awards program.

Employee recognition programs are often combined with reward programs, though they serve different purposes. The reward is the item given; recognition is the publicizing, announcing, or celebrating of the person, action, or reward. Recognition is a human resource tool used to increase morale and employee performance, and to meet work goals and initiatives while promoting work values. This makes targeting the desired behaviors as important as the form of recognition.

Rewards can include merit-based pay raises, monetary compensation, and other awards like certificates and plaques. Create awards and recognition for regular job duties, and tailor some for following security protocols, to increase motivation in that area. These recognitions help improve motivation to be watchful and involved in maintaining security.

To reinforce awareness and engagement in security efforts, airports can also include a recognition program such as Massport's SAFE Campaign.

**Massachusetts Port Authority (Massport) Security Awareness for Everyone (SAFE) Campaign**
SAFE identifies employees who have demonstrated exemplary security awareness in their daily jobs at Boston Logan International Airport (BOS). Selected employees and their photos are featured in a series of campaign posters on display at the airport. The award recipients are recognized at a formal ceremony officiated by Massport executives. Frontline employees are considered for recognition for exemplary security awareness based on the following:

- Reporting a potential or actual security incident
- Preventing or detecting a potential or actual security incident
- Performing an action resulting in improved response and resolution by public safety
- Demonstrating exceptional support of airport security initiatives
- Demonstrating security awareness or constituting instructional value

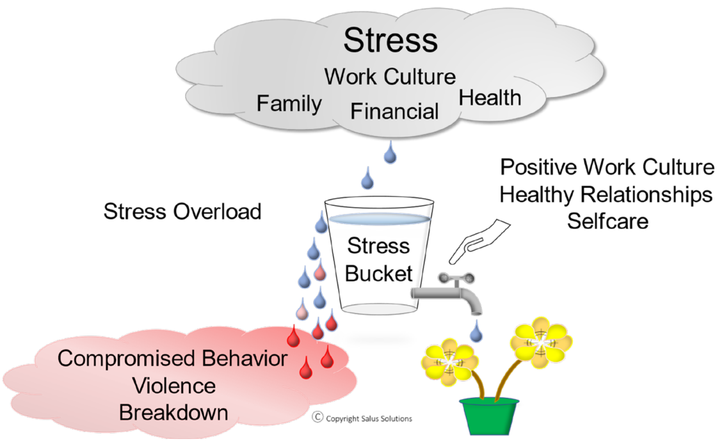
SAFE is a great example of how recognition and rewards can increase awareness, engagement, and participation. Examine the reward system, including pay raises and promotions, so ensure it is fair and achievable, and is free from favoritism and bias. This can raise motivation and job satisfaction. Massport reports that the return on this investment has been outstanding while having a minimal budgetary impact. Programs such as SAFE reward performance and motivate employees on individual and group levels.

## 5.2 Mental Health Treatment and Counseling

The Center for Development of Security Excellence, Department of Justice, FBI, and others agree that early intervention with employees in distress is the preferred strategy for mitigating insider threats. Employee stressors usually manifest in undesirable behaviors and though they are noticeable, they are not always reported. Insider threats often begin with stressors building in a person's circumstances until they reach a breaking point. Both employment and home stress can lead to emotional exhaustion.

Encourage self-reporting by individuals. It is important to note negative events do not always indicate an increased risk of an insider threat, especially if they self-report. An individual who is able to verbalize his or her feelings when under stress, or is dealing with a negative event, is using positive coping mechanisms. Early reporting with a goal of empathic engagement can then lead to counseling or therapy, which help people deal with stress and emotions in healthy ways. As stress is reduced, so is risk.

Figure 8. Stress Management



Airport operators can evaluate the accessibility and quality of their Employee Assistance Programs (EAP). Such programs normally assist with such concerns as childcare and transportation, but it is important to also provide for mental health treatment and counseling services and other forms of support and resources that can reduce personnel stressors. The existence of EAPs can also help reduce personnel turnover.

Airports can refer to the Safe Skies guidebook *PARAS 0033 Mental Health and Airport Security* (publication anticipated in December 2021) for guidance of how to implement Mental Health First Aid and other interventions. This guidance provides employees with the tools to identify persons suffering from mental health issues, understanding that person, and the appropriate response.

## 5.3 Reducing Personnel Turnover

Employees generally remain in their jobs if they have job satisfaction, social connection, meaning and purpose, and reasonable autonomy. Job satisfaction is higher when they have fair pay and reasonable hours, personal safety, job security, and opportunities for awards, raises, and recognition. When these conditions falter, people leave their jobs at higher rates.

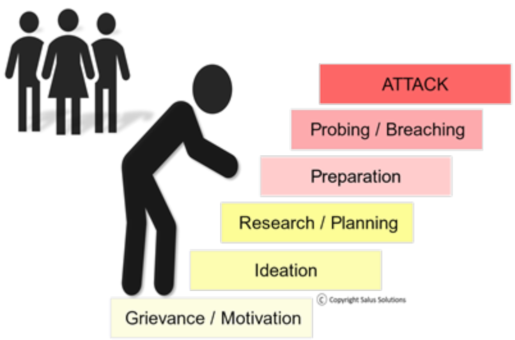
High turnover increases insider threat risk and puts stress on management to continually retrain employees about security and to integrate new employees into a team environment. When an employee leaves an airport, their insider knowledge goes with them. It can then more likely be transferred to others, either knowingly or unknowingly. In addition, being understaffed negatively affects the stress level of the remaining workers who are charged with additional work.

High turnover can also affect security. For example, high turnover among airport screening officers increases the proportion of novice screeners who lack expertise. Turnover also increases the possibility of leaked screening techniques, which makes it easier to find ways to circumvent them. Employees who leave disgruntled still have contacts within the airport environment, and they may attempt to seek revenge through manipulation of their previous relationships. An insider threat program should include monitoring and reporting initiatives for former personnel who leave their agency or organization and reveal sensitive information.

## 5.4 Addressing Workplace Harassment

Intimidating or harassing behavior can happen in any work environment. If managers fail to take immediate corrective action, offer ineffective resolutions, or remain silent, they can appear to be accepting of the negative behavior. Airports need to take a complete view of the incident, take corrective action, and respond systemically to send a message to workers that intimidation and harassment will not be tolerated.

Figure 9. Escalation of an Insider Threat



Each step is an opportunity to interrupt the insider threat

Workplace victimization can take active and passive forms, sometimes adding to difficulty in identifying an issue. The mistreatment of an employee can create an environment that breeds insider threats because of the motive of revenge against the employer and employees. Witnesses' perceptions of mistreatment are related to higher levels of stress and workplace negativity. Negative work environments can cause lower job satisfaction, so a supportive management style is important. A coercive or authoritarian management style demeans workers and encourages supervisors to use intimidation and fear-based leadership. Laissez-faire management is unlikely to respond at all and is usually ineffective.

Leadership and management should be actively aware of victimization among employees and addressing any issues before victims become disgruntled and a potential insider threat arises. Implement measures to monitor employees' reactions to management responses to intimidation. When the actions of an antagonist are addressed immediately and effectively, employees may feel safer, and the corporate position of zero tolerance for harassment or intimidation is thereby reinforced.

Having effective policies and procedures in place reduces fear-induced silence, victim-blaming, or siding with abusers who might feel mobbed. Create metrics to analyze incident behavior, employee perception, and leadership response. This creates opportunities to address a situation before an employee begins to seek revenge against individuals or the organization.

# SECTION 6: ENFORCING RULES, REGULATIONS, AND SANCTIONS

Information in this section aligns with ASAC Focus Area 6, Governance and Internal Controls

**Management must attend administrative violation meetings**

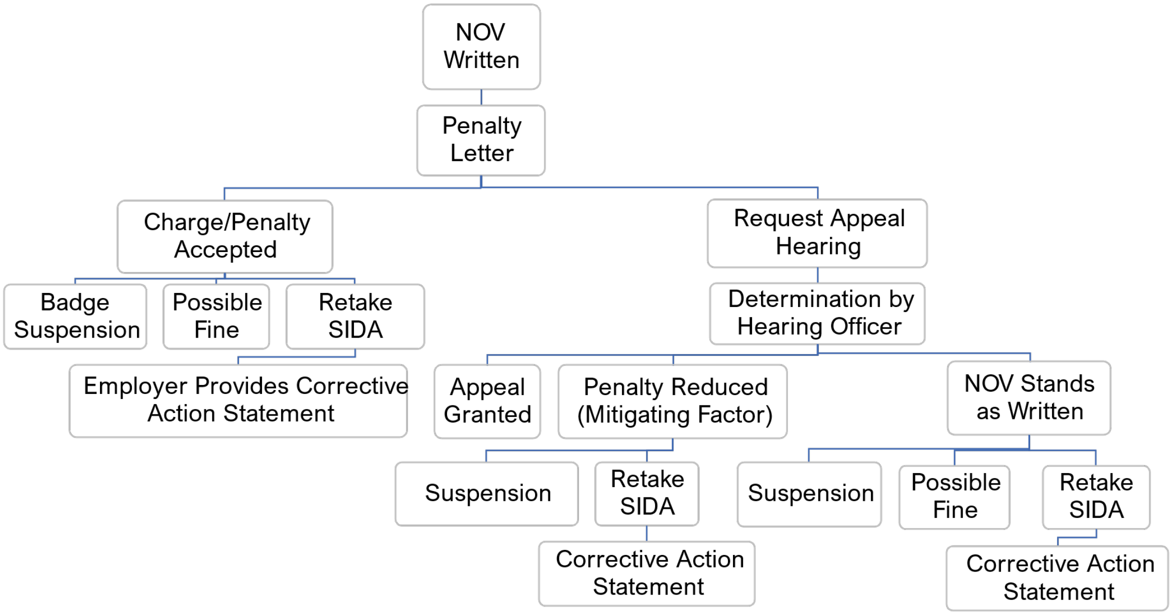
Airports in the U.S. are heavily regulated by multiple government agencies, including the FAA and DHS. Airports use regulations to develop their own policies, procedures, rules, and sanctions specific to their operations. A clearly defined, progressive discipline program provides for initial documentation, tracking of any additional future violations, and use of a violation as a training tool. A tiered progressive disciplinary approach, focusing on using violations as learning opportunities for training, helps employees to understand security concerns by providing a true account of an issue and the response to it. Clear expectations, strict adherence to policies, and fair enforcement reinforce the importance of security awareness and compliance.

## 6.1 Badge Holder Responsibilities

Airport badge holders are the first and best line of defense against an insider threat, because they know what is normal and not normal for their work areas. The responsibilities of badge holders are clearly defined by 49 CFR § 1540 Civil Aviation. Badge holders must not compromise or circumvent security measures, and they must comply with inspection and screening regulations. Badges are the property of the airport operator; however, once issued, control of a badge is the responsibility of the holder. The airport operator has the authority to revoke a SIDA badge, and it must be surrendered to the operator immediately upon demand. Airport employees must understand the level of accountability and responsibility when being issued a badge.

Airport operators can develop an appropriate Notice of Violation (NOV) process, as shown in Figure 10.

Figure 10. Notice of Violation Administrative Process



The positions and persons who can issue badge use violations should be defined, and can include law enforcement, airport operations personnel, and security officers. Various penalties can be developed to meet the level of violation that occurs, and they can include badge suspension, monetary fines, or both. For additional information, *PARAS 0020 – Strategies for Effective Airport Identification Media Accountability and Control* guidebook provides detailed strategies for consideration.

Regardless of any penalty, violating individuals should be required to attend security training again. Airport operators have found that requiring employees' supervisors to attend the training as well has a greater impact on reducing repeat offenses. Punishment should escalate for multiple violations.

An appeals process should be established to ensure each situation is evaluated, and accused employees are given an opportunity to defend themselves. Depending on the size of an airport, one or more appeals officers can be identified.

By reviewing NOVs issued monthly, airport operators can identify weaknesses that need correction and ensure they cannot be exploited by an insider threat. Reviewing incidents resulting in NOVs is highly effective in training, because they apply directly to the airport rather than being a hypothetical example.

### 6.1.1 Sanction Strategies

Maintaining a clearly defined progressive discipline program allows for documentation of violations and for use of that information as a learning tool. In some cases, the airport operator may consider having the employee's supervisor or corporate management involved in the progressive discipline process. Airport operators can also refuse to issue or re-issue a badge to an employee. While the airport operator cannot terminate a stakeholder's employee, they do have the right to refuse access to restricted areas. Some airports will not re-issue a badge to a person who has lost three badges.

As each airport is unique, so are their tenants and airlines. Each airline or company working on the airfield has its own security culture and may reinforce the airport's policies differently. Additionally, company turnover rates affect the type and number of repeated violations. For example, airports with more contract personnel may have more employee turnover and more violations of the same type than an airport where ramp employees work for the airport.

A fee could be assessed for replacing a lost or damaged badge, depending on the reasons for damage. The damage fee should be less than the fee charged for a lost badge. In instances when a badge is reported stolen, it is suggested the replacement fee be charged unless a police report was submitted. Consideration can be made for a full or partial refund if a lost or stolen badge is returned prior to expiration. Additionally, a tiered fee schedule deters repeat offenders. For example, the first replacement badge fee might be $25, the second $50, and the third could be $100. Airport operators may consider refusing to issue a new badge to applicants who have lost their badge multiple times. Each airport will determine the appropriate levels for fines based on the cost of badges they use and on their badge replacement schedule. The amount of time that passes between instances of lost badges may also affect the fine charged. For example, use of the $25-$50-$100 schedule may apply well may be unnecessarily harsh for badges lost with a ten-year span between events.

Other sanction strategies include the following:

- Weekly or monthly training alerts to discuss recent incidents or trends in mistakes or sanctions
- Mandatory administrative meetings for the employee's direct manager and senior manager
- Mandatory retraining of employees and their direct supervisors
- Suspension of airport access for a period of time, or termination

Use each violation as a learning opportunity for the employee, and allow employees to assist in developing a security-minded culture. Clear expectations are essential to ensure that strict, but fair, enforcement of rules and the issuance of violations do not have a negative impact. Training and developing good relationships and communication allow the airport community to build an understanding of the importance of security regulations.

## 6.2 Escorting Requirements

Escorts must be easily differentiated from other personnel. It is essential to be able to quickly identify individuals who can escort others versus those who cannot. Airport operators can improve visual identification factors in many ways, such as badge design, color, and decals.

Establish clear and specific rules concerning access points, allowable time, and number of persons escorted. Requirements to define include:

- Purpose and circumstances when escorting is allowed
- Visual, verbal, and other controls
- Ratio of escort to persons under escort
- Penalties for violations
- Process for transfer of escort
- Contractor tool accountability procedures

Airport operators should use escort request forms and an escort log to monitor suspicious trends. A computer-based portal may be an option for these forms and logs.

Random inspections should be conducted to ensure escorted personnel are in the location requested and have not exceeded the time duration. Keeping a record of entry and inspection of escorted individuals and vehicles allows tracking of suspicious access activity. This can be accomplished by only allowing the escort through manned points of access.

Each airport must consider the need for special escort rules concerning transient crew, aircraft mechanics, and emergency response personnel based on variables such as common-use gates, leased spaces, and the overall terminal and airfield layout.

*PARAS 0035 – Synthesis of Escorting Privileges and Escorting Practices* (available May 2021) provides additional details on policies and controls for escorting.

## 6.3 Challenge Procedures

Pursuant to regulations, when individuals are in a SIDA area, their badges must be displayed above the waist on their outermost garment. Employee SIDA training provides the types of badges used at the airport and how to identify the proper security levels including escort privileges, if allowed. Individuals observed without proper credentials for the area must be challenged. Consistently following challenge procedures helps to detect and deter potential insider activity.

Many airports have created a positive approach to SIDA challenges by using rewards. Employees of the airport operator walk in areas where SIDA display is required but without displaying proper credentials. Employees who properly challenge them, asking to see their SIDA badge, receive rewards such as a gift card for food or beverage at the airport, or a certificate or letter of appreciation. With this approach, the paradigm shifts from “gotcha” to praise and reward, resulting in an increase in challenges.

Failure to challenge individuals not displaying their SIDA badges is a violation, but the emphasis of the program is instead on the reward. This reward program can be expanded by allowing for nominations for security-minded behavior or for stopping a potential security risk. Conduct award ceremonies periodically. Acknowledgements can also be included in newsletters, posted on the airport intranet, or depending upon circumstances, on an external website. Employee feedback in some programs indicates that knowing they are part of the security culture and receiving recognition for following the rules is more meaningful than receiving a monetary reward.

In training, instruct employees to avoid placing themselves in physical danger, but instead report any suspicious person and attempt to continuously watch the person until responding officers arrive.

# SECTION 7: CONCLUSION

Insider threats present a complex challenge for airports because they can emerge from any area of the airport environment. While direct employees are the most obvious potential threats, all contractors and vendors who access airport property have the potential to become an insider threat.

The factors motivating someone to engage in criminal activity against people or organizations are myriad and typically personal in nature. Motivation can spring from a wide range of life experiences, including work, family, and financial stressors. Any suspicious or unusual behavior should be reported immediately to airport security, tip lines, law enforcement, airport operations or the airport's Insider Threat Working Group.

Because of the difficulty in identifying insider threats before they act, detection strategies are paramount. Airports should regularly re-evaluate their detection strategies. Integrating technology, personnel, and processes through all aspects of daily operations offers the best possibility of identifying potential threats, and addressing them prior to an incident. Establishing layers of deterrence and detection is the best strategy.

Cybersecurity tools detect access to electronic assets; cameras enable observation; electronic door locks, badges, and chip keys provide access control; and pressure plates and sensors detect unauthorized presence and movement. Interconnecting these technologies with a system that can assimilate and analyze the each device's output provides an extremely powerful tool for detecting security breaches in real time.

Train all airport staff to understand how and why a person becomes an insider threat. Teach them how to detect and mitigate potential insider threat activity. Such training builds a culture of insider-threat awareness. Personnel can more readily alert authorities about unusual behavior when they have a thorough understanding of potential threats.

Another strategy for combatting insider threats is sharing information with other agencies. Collaboration is key for a successful insider threat team. Multi-agency cooperation and sharing of technology and information are critical. Airport operators can facilitate information sharing between agencies, industry, and key stakeholders. TSA's ASAC recommends developing a Hub, to bring together agencies and stakeholders having roles in combatting insider threats. In sharing information between agencies, airports should consider the legal and ethical obligations to privacy, especially for airport employees, the traveling public, and other stakeholders.

Airport operators can meet with appropriate law enforcement agencies to determine the possibilities for exchanging information for criminal investigations, incident response, intelligence sharing, and insider threat cases. In addition to law enforcement, other stakeholders can be strong allies in combatting insider threats. Many airlines have established insider threat programs in their own companies. Therefore, their participation in a working group or Hub can yield valuable and timely information.

By employing the strategies and practices described in this guidebook, airports can establish or re-enforce a security-minded culture. A strong culture starts with clear leadership and supports open dialogue for identifying and reporting insider threats. The overall objective is to identify suspicious actions within organizations and to determine what actions to take upon identifying a threat.

## REFERENCE MATERIAL

Listed in this section are guidance documents and sources of information that discuss topics related to insider threats. These materials were used in the research for this guidebook.

*PARAS 0001 – Criminal History Records Checks (CHRC) and Vetting Aviation Workers Guidebook*

*PARAS 0003 – Enhancing Communication & Collaboration Among Airport Stakeholders*

*PARAS 0006 – Employee Inspections (Synthesis Report)*

*PARAS 0008 – Findings and Practices in Sharing Sensitive Information (Synthesis Report)*

*PARAS 0009 – Guidance for Security Management Systems (SeMS)*

*PARAS 0010 – Guidance for Protecting Access to Vital Systems Impacting Airport Security*

*PARAS 0016 – Airport Security Vulnerability Assessments*

*PARAS 0019 – Employee/Vendor Physical Inspection Program Guidance*

*PARAS 0020 – Strategies for Effective Airport Identification Media Accountability and Control*

*PARAS 0033 – Mental Health and Airport Security* (in progress)

*PARAS 0035 – Synthesis of Escort Privileges and Escorting Practices*

ASAC Working Group on Airport Access Control Final Report (April 2015)

ASAC Report on Insider Threat (July 2018)

ASAC Report: Review of TSA’s Insider Threat Advisory Group Findings (March 2019)

ACRP Synthesis 113: Airport Workforce Programs Supporting Employee Well-Being

ACRP Report 140: Guidebook on Best Practices for Airport Cybersecurity

ALEAN Airport Law Enforcement Agencies Network

Airports Council International North America. Addressing Insider Threat Handbook, First Edition. 2019. https://store.aci.aero/product/addressing-insider-threat-handbook/.

GAO Report to Congressional Requesters. Aviation Security: TSA Could Strengthen Its Insider Threat Program by Developing a Strategic Plan and Performance Goals

Airport Cooperative Research Program, Report 140: Administration Guidebook on Best Practices for Airport Cybersecurity

House Homeland Security Committee Majority Staff Report. America’s Airport: The Threat from Within. February 2017

"FBI Counterintelligence: The Insider Threat. An introduction to detecting and deterring an insider spy" 2014-02-10. Retrieved 2014-03

Insider Threat: Prevention, Detection, Mitigation, and Deterrence, from Sabotage, Spying, and Theft, 15 March 2006

National Insider Threat Task Force, “Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards, 2017.

National Insider Threat Task Force, “Protect Your Organization from the Inside Out: Government Best Practices,” 2016.

National Insider Threat Task Force, Insider Threat Program: Maturity Framework, 2018. https://www.dni.gov/files/NCSC/documents/nittf/20181024_NITTF_MaturityFramework_web.pdf.

National Insider Threat Task Force. “Insider Threat Guide: A Compendium of Best Practices to Accompany the National Insider Threat Minimum Standards. (2017): 7

Airports Council International (ACI), Addressing Insider Threat Handbook, First Edition 2019

Ponemon Institute, “2020 Cost of Insider Threats: Global Report,” 2020.

The Public-Private Analytic Exchange Program, Aviation Insider Threat Team, “What We Know, Our Findings, and What We Recommend,” 2017.

Deloitte, “Disrupt Aviation: Part 1: Unpredictable and Malicious Threats,” 2015.

Deloitte, “Top 10 considerations: Building an insider threat mitigation program, 2016.

Center for Development of Security Excellence, “Conduct Insider Threat Training,” Insider Threat Job Aid for Industry. http://www.cdse.edu/catalog/insider-threat.html.

Center for Development of Security Excellence, “Insider Threat Toolkit,” https://www.cdse.edu/toolkits/insider/index.php.

Center for Development of Security Excellence, “Potential Risk Indicators: Kinetic Violence: What is the “something” we should be looking for?” https://www.cdse.edu/documents/cdse/potential-risk-indicators-kinetic-violence-jobaid.pdf.

The Public-Private Analytic Exchange Program: Aviation Insider Threat Team 2017, “Aviation insider threat: what we know, our findings, and what we recommend,” 2017: 10.

The Public-Private Analytic Exchange Program: Aviation Insider Threat Team 2017, “Aviation insider threat: what we know, our findings, and what we recommend,” 2017: 4-6, 10.

Transportation Security Administration, “Insider Threat Awareness: ICAO Global Aviation Security Symposium,” 2018.

Transportation Security Administration, “Report of the Aviation Security Advisory Committee on Insider Threats at Airports,” 2018: 3.

Transportation Security Administration, “SIDA Airport Security, Fiscal Year 2017 report to Congress” 2018.

US Department of State, “The American Liaison Network: A Resource and Model for Crisis Communication,” 2016.

U.S. Department of Energy, The Threat Among Us: Insiders Intensify Aviation Terrorism, Aug 2016

# APPENDIX A: CHECKLISTS, FORMS, AND ILLUSTRATIONS

In this appendix are several checklists, forms, and illustrations. They can be printed and filled out, or used as references. Some items may be useful to post where employees can be reminded of some of the objectives and behaviors related to mitigating insider threats at airports.

All graphics and other tools are available for download in print quality at www.Salus.Solutions/Library.

## Insider Threat Working Group Checklist

This checklist is useful for planning the development and use of an Insider Threat Working Group or Hub. As described in this guidebook, a working group is informal and usually comprises a group of stakeholders to gather information about insider threats at an organization or facility. As a working group evolves, it may be formalized in a Hub, to include a budget and authorities for planning mitigation of insider threats.

### Insider Threat Working Group or Hub Planning Checklist

#### Initial Contact

| Objectives Activities and Task | Owner | Date Completed |
|---|---|---|
| Select Senior Official<br>(Agency Senior Official / Working Group Organizer) | | |
| Stakeholders<br>(Identify Agencies and Stakeholders to Participate) | | |
| Strategic Overview<br>(Prepare and send strategic overview to agencies and stakeholders asking them to identify a senior level official for kick-off meeting) | | |
| Reserve Meeting Space / Virtual Meeting<br>(Identify and reserve meeting space. Identify and reserve back-up location. Ensure both spaces are suitable for confidential discussions. Identify date and time.) | | |
| Invitations<br>(Organize list of senior leaders, schedule kick-off meeting, and send invitations, include date, time, primary and secondary locations) | | |
| Agenda<br>(Develop kick-off meeting agenda) | | |
| Confirm Attendees<br>(Send meeting reminder and confirm RSVP list) | | |
| Prepare Materials<br>(Prepare materials for meeting) | | |

#### Objectives

| | | |
|---|---|---|
| Mission and Strategy<br>(Create a mission statement and strategy for the group) | | |
| Talking Points<br>(Create talking points that reflect the mission and strategy) | | |

| | | |
|---|---|---|
| Prepare Materials<br>(Prepare materials for meeting) | | |
| Critical Assets<br>(Identify critical assets, processes, and resources to protect) | | |
| Vulnerabilities<br>(Identify vulnerabilities in the assets, processes, and resources) | | |
| Sources of Threats<br>(Identify sources of threats) | | |
| Policies<br>(Identify applicable policies) | | |
| Identify Subject Matter Experts<br>(Legal, Financial, Technology, Mental Health, Medical, Law Enforcement, Regulatory) | | |
| Nondisclosure Agreements<br>(Create non-disclosure agreements as necessary) | | |
| Memorandum of Agreement<br>(MOAs to support Insider Threat Working Group for staff, resources, and information and data sharing) | | |
| Create Procedures<br>(Create procedures for data and analytics, planning, collecting, analysis and evaluation, investigative referral and coordination, development of strategic framework, and what data can be shared, how will it be shared, storage platform, and analytics) | | |
| Privacy Requirements<br>(Identify privacy requirements and procedures) | | |
| Legal Requirements<br>(Identify legal requirements and procedures) | | |
| Union/Workforce Requirements<br>(Identify labor requirements and procedures) | | |
| Training and Awareness Programs<br>(Decide course of action for training and awareness) | | |
| Mental Health Concerns<br>(Decide procedures for address mental health needs) | | |
| Frequency of Meetings<br>(Create a regular meeting schedule) | | |
| Procedures and Forms for Reporting and Evaluation<br>(Create procedures and forms for reporting, report preparation, and case review) | | |
| Staffing and Resource Obligations<br>(Identify and request necessary staffing and resources) | | |
| Budget<br>(Create budget, request approvals) | | |

## Stakeholders in an Insider Threat Working Group or Hub

This list comprises numerous groups and individuals to consider as stakeholders in a working group or Hub. Some may be directly involved in forming the organization, while other stakeholders are beneficiaries of the work without being directly involved in developing or maintaining it.

It is of critical importance to engage all stakeholders in developing the group. By referring to this list, organizations are less likely to miss vital components of an airport ecosystem.

### Potential Stakeholders in an Insider Threat Working Group or Hub

- Air Carriers
  - Commercial Airlines
  - Cargo (FedEx/UPS/DHL)
  - General Aviation Fixed Based Operator
- Airport Organizations
  - Airport Fire and EMS
  - Airport Security Director / Dep. Security Director
  - Airport Police
  - Mental Health Professional
- Federal
  - FAA
  - TSA
    - Federal Air Marshal Service (FAMS)
    - Federal Security Director
  - FBI (supervisor or Airport Liaison Agent)
  - CBP
  - ICE

## Observed Behavior Report Form

This section contains suggested items for use in an airport's reporting form to collect information about suspicious behavior observed by individuals in your organization. Instruct employees completing this report that it is important to provide clarity and context, and that the report should be credible (see Section 4.2.1 of this guidebook). The completed report is then evaluated by the Insider Threat Working Group or similar group and assessed for further action.

Before a report is ready for evaluation, it should first be prepared for presentation. This involves analyzing the report to ensure all information (so far as it is known) is included in the report. Check for clarity, context, and credibility, and identify any statements of bias or opinion. Presentations of reports should identify gaps in the information and indicate what information is needed to verify statements. The preparation should also identify alternative explanations for the behavior.

The Privacy Act and Whistleblower Protection Act are federal laws, and civil liberties are broadly protected in the U.S. Constitution. Care must be taken to protect these rights when making a report on suspicious behavior. Any violations of these rights in deterrence, prevention, detection, and response actions can weaken legal actions taken later against a true insider threat.

# Observed Behavior Report Form

Insider Threat Working Group

## To be Completed by the Reporter

**Submit Report To**

□ Tip Box
□ Tip Phone Line
□ Email
□ Person-to-Person

**Purpose**

*This field should contain airport-specific general information about the insider threat program and the purpose of reporting concerns.*

**Anonymity Desired?**

□ Completely anonymous
□ Known only to the Insider Threat Working Group and investigators
□ Known to the public

**Date/Time of This Report**

Date

Time

**What Behavior(s) or Statement(s) was Observed?**

What specific action occurred?

What specific statements were made?

*Reviewer's Comments*

**Has the Individual Done or Said This Before?**

When?

Where?

Describe

*Reviewer's Comments*

**Information About the Individual**

Name

Company/Department

Male/Female

Height

Weight

Estimated Age

Clothing

*Reviewer's Comments*

**In What Context did the Behavior or Statements Occur?**

Date

Time

Place/Location

Mood/setting

Number of People

*Reviewer's Comments*

**Individuals Present at the Time of the Observation or Statement**

1st Person

Name

Rank, Job Title

2nd Person

Name

Rank, Job Title

3rd Person

Name

Rank, Job Title

Additional Persons (Name, Rank, Job Titles)

*Reviewer's Comments*

**Did Something Prompt or Provoke the Behavior? What Happened Immediately Before or After the Behavior?**

Yes or No?

Explain

*Reviewer's Comments*

**What Additional Information Might be Important to Know?**

Explain

*Reviewer's Comments*

**What are Possible Alternative Explanations for the Overserved Behavior or Statements?**

1st Possible Explanation

2nd Possible Explanation

3rd Possible Explanation

*Reviewer's Comments*

**About You**

Name (optional)

Telephone Number (optional)

Email Address (Optional)

Job Title (optional)

Have you Recently Experienced Any Positive or Negative Life Events?

*Reviewer's Comments*

**What is Your Relationship to the Individual?**

How often do you see the individual?

For how long do you see the individual?

Where do you normally see the individual?

Describe the quality of your relationship with the individual

*Reviewer's Comments*

## To Be Completed by the Insider Threat Working Group

**Is this Report Ready for Review?**

Yes/No

What is missing?

**Insider Threat Working Group Evaluation of This Report**

Explain

**Which Physical Areas of The Airport Does This Affect?**

Explain

**Which Departments of the Airport Does This Affect?**

Explain

**Which Stakeholders Does This Affect?**

Explain

**Who Needs to Know About This Report?**

1st to Notify

Accomplished Date and Time:

2nd to Notify

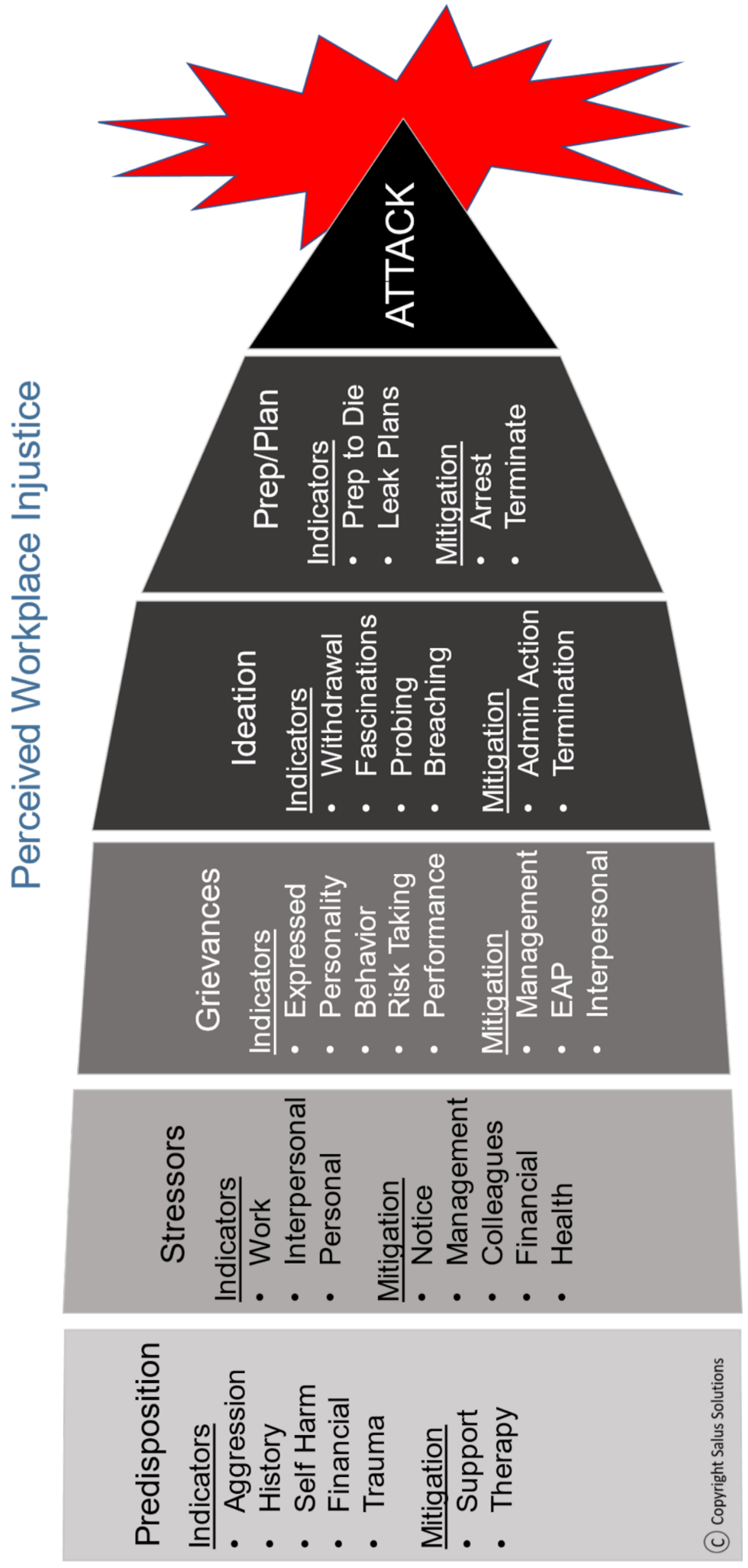
Accomplished Date and Time:

3rd to Notify

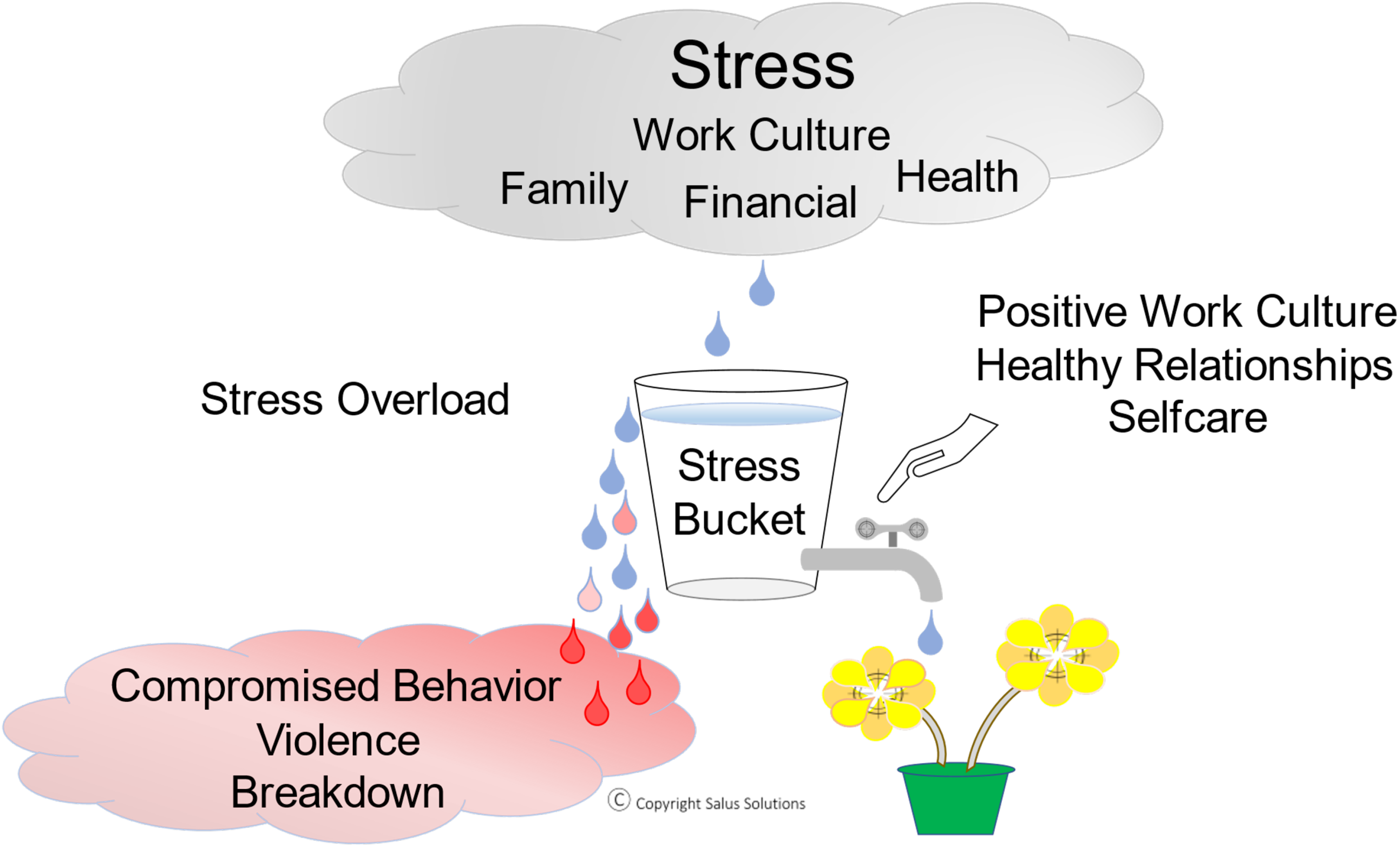
Accomplished Date and Time:

**Next Steps**

## Illustrations



# Stress Management



Stress

Work Culture

Family Financial Health

Stress Overload

Stress Bucket

Positive Work Culture

Healthy Relationships

Selfcare

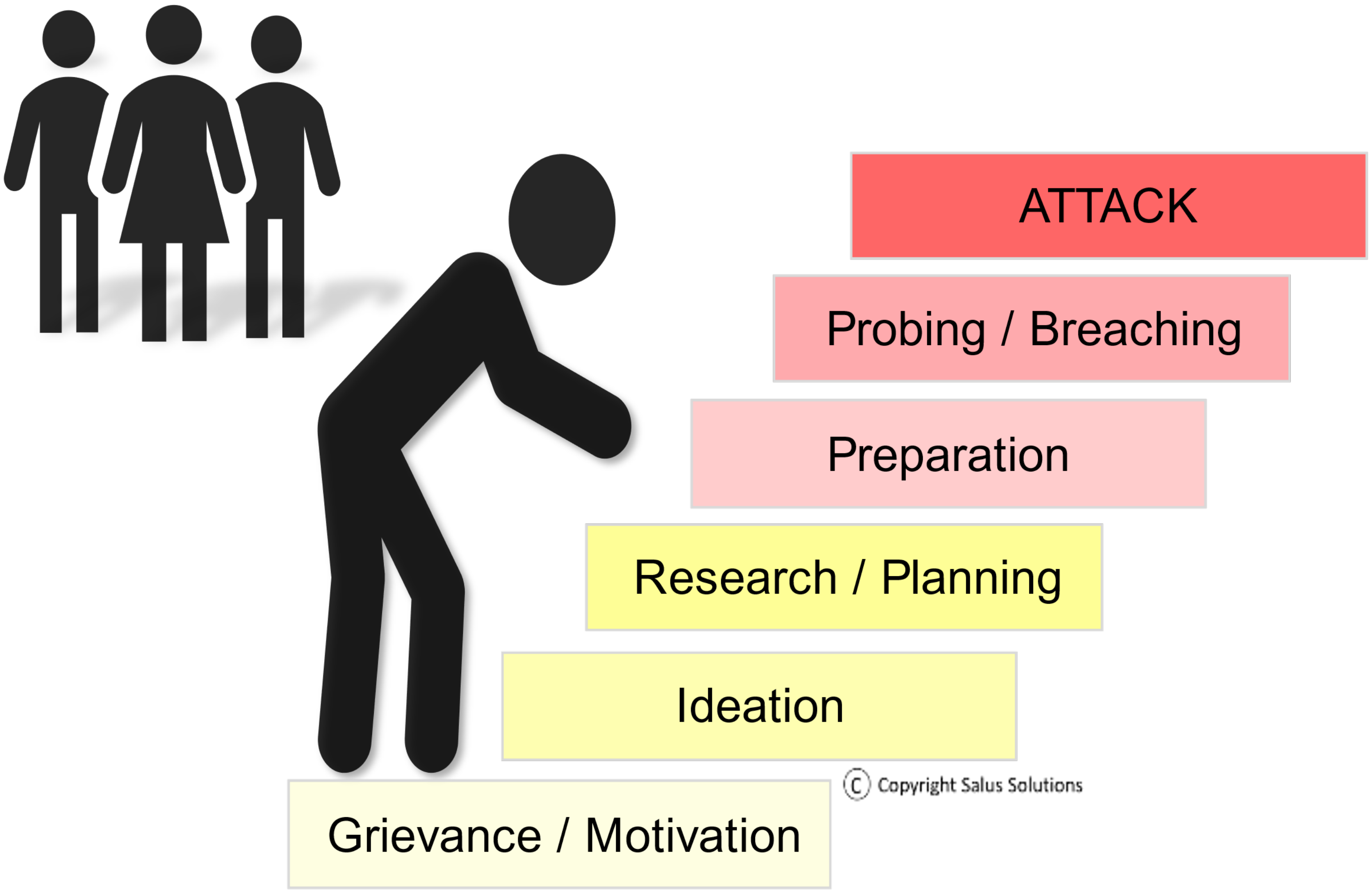
Compromised Behavior

Violence

Breakdown

Ⓒ Copyright Salus Solutions

# Escalation of an Insider Threat



Each step is an opportunity to interrupt the insider threat

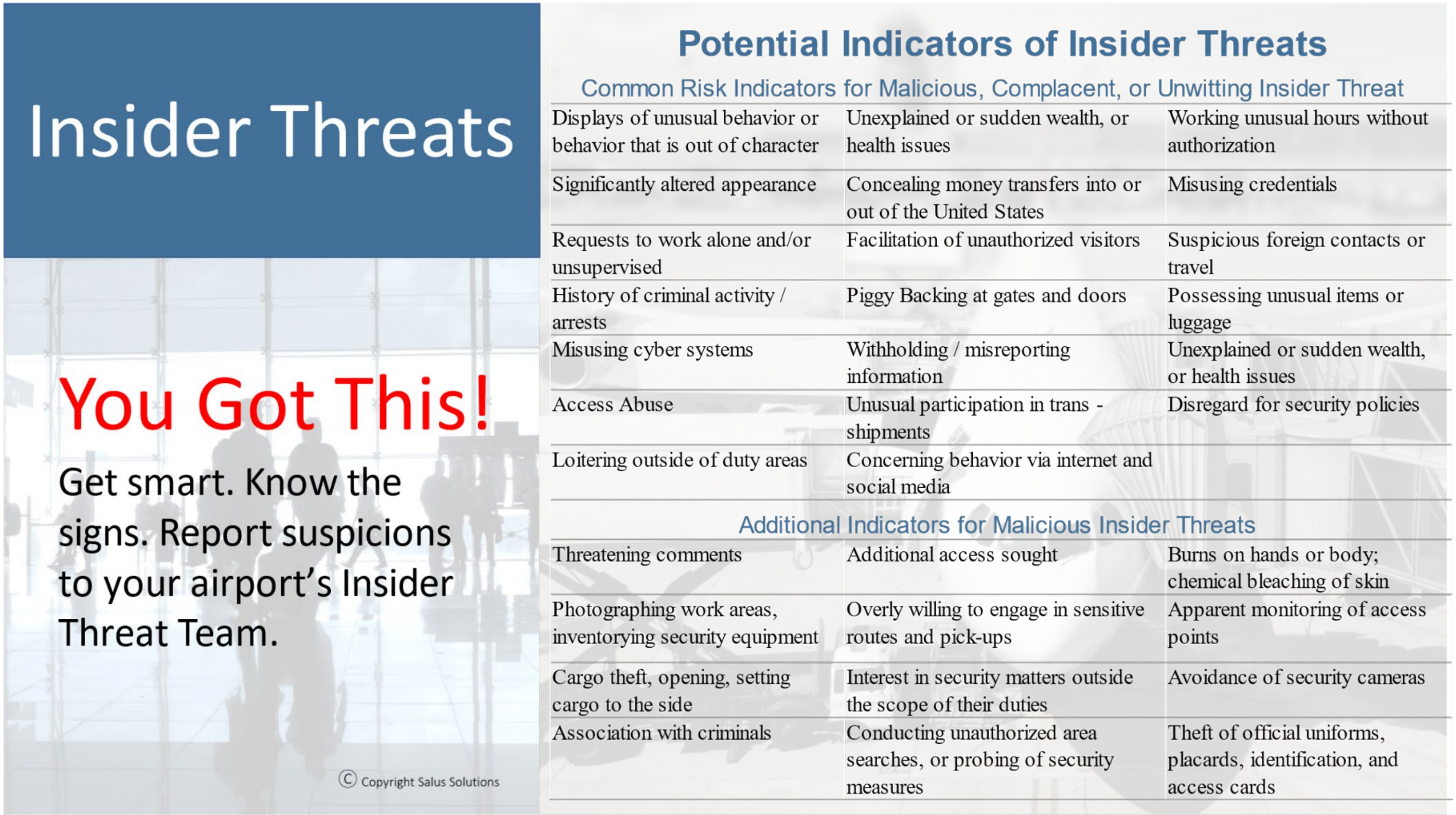
# Insider Threats

## You Got This!

As a member of the aviation community, it's your responsibility to ensure we are safe from insider threats.

Get smart. Know the signs.
Report suspicions to your airport's Insider Threat Team.

Make a Report:



# Insider Threats

You Got This!

Get smart. Know the signs. Report suspicions to your airport's Insider Threat Team.

## Potential Indicators of Insider Threats

### Common Risk Indicators for Malicious, Complacent, or Unwitting Insider Threat

| | | |
|---|---|---|
| Displays of unusual behavior or behavior that is out of character | Unexplained or sudden wealth, or health issues | Working unusual hours without authorization |
| Significantly altered appearance | Concealing money transfers into or out of the United States | Misusing credentials |
| Requests to work alone and/or unsupervised | Facilitation of unauthorized visitors | Suspicious foreign contacts or travel |
| History of criminal activity / arrests | Piggy Backing at gates and doors | Possessing unusual items or luggage |
| Misusing cyber systems | Withholding / misreporting information | Unexplained or sudden wealth, or health issues |
| Access Abuse | Unusual participation in trans - shipments | Disregard for security policies |
| Loitering outside of duty areas | Concerning behavior via internet and social media | |

### Additional Indicators for Malicious Insider Threats

| | | |
|---|---|---|
| Threatening comments | Additional access sought | Burns on hands or body; chemical bleaching of skin |
| Photographing work areas, inventorying security equipment | Overly willing to engage in sensitive routes and pick-ups | Apparent monitoring of access points |
| Cargo theft, opening, setting cargo to the side | Interest in security matters outside the scope of their duties | Avoidance of security cameras |
| Association with criminals | Conducting unauthorized area searches, or probing of security measures | Theft of official uniforms, placards, identification, and access cards |