ASAC
AVIATION SECURITY ADVISORY COMMITTEE

July 19, 2018

Honorable David Pekoske
Administrator
Transportation Security Administration
601 12th Street South
Arlington, VA 20598

Dear Administrator Pekoske:

At its meeting on July 17, 2018, the Aviation Security Advisory Committee (ASAC) formally approved the Report on Insider Threat originally sent to you as an Advance Copy on June 21, 2018. For the record, a final copy of the Report is attached hereto. There are no substantive changes from the original submission.

In order to plan for future ASAC work on the insider threat issue, I would like to request a short meeting some time in the next few weeks to discuss the next phase of this project, including your expectations and projected time lines. The next meeting of our Insider Threat Subcommittee is scheduled for August 29 so a meeting before then would be extremely helpful.

Thanks very much.

Sincerely yours,

Steve Alterman
Chairman

Cc: Victoria Newhouse, ASAC Executive Sponsor
Tamika Elhilali, ASAC DFO
Dan McCann, Insider Threat Subcommittee DFO
Serge Potapov, TSA Co-chair, Insider Threat Subcommittee
Frank Capello, Industry Co-chair, Insider Threat Subcommittee

REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE

ON INSIDER THREAT AT AIRPORTS

Table of Contents

INTRODUCTION

In a letter to Stephen Alterman, Chairman of the Aviation Security Advisory Committee (ASAC), dated March 23, 2018, TSA Administrator David P. Pekoske requested that ASAC look at the security threat posed by airport insiders – aviation workers with privileged access to restricted areas of our Nation's Airports, and thereby to commercial aircraft.

The request envisioned two parts to the initiative with the first part of the initiative to be delivered within 60 to 90 days and focus on a holistic report around the concept of insider threat with the following topics for consideration:

- Definition of "Insider Threat" from an industry perspective;
- Comparative analysis of leading domestic companies' insider threat initiatives, and;
- Analysis of at least one international program (e.g., Israel, AIRPOL[1] Amsterdam Airport Schiphol); and,
- Recognized practices that are common among mature insider threat programs.

In response to this request, ASAC convened its Working Group on Airport Access Control, and identified sub-working groups, or teams, to address the four separate elements of the request.

This report consolidates the teams' research in response to the Administrator's first request.

Response to future related requests from the Administrator will likely be drafted by the newly forming ASAC Subcommittee on Insider Threat.

DEFINITION OF INSIDER THREAT

Approach

The working group collected Insider Threat Definitions and Policy Scope (see Appendix A) from multiple sources, including government agencies, trade and other professional organizations, as well as private entities and unattributed sources. The purpose of this initial effort was to review and assess the applicability of existing definitions to collectively define insider threat from an aviation industry perspective.

The working group discussed the scope of what should be considered in defining insider threat, but recognized that individual entities within the aviation industry are likely to adhere to a broader meaning, covering a wide variety of risks to include theft of intellectual property or sensitive data, sabotage of systems, violence in the workplace, property damage, etc.

[1] AIRPOL, a coordinating body of law enforcement units at European airports is currently developing an Insider Threat Guidebook and training course.

Considering that TSA was created after September 11, 2001, to prevent similar terrorist attacks into the future, the working group concluded that an overly broad definition was inappropriate. Instead, the definition should align TSA's mission of protecting the nation's transportation systems to ensure freedom of movement for people and commerce, by focusing efforts on criminal activity, terrorism, or other illicit actions which inflict "significant" harm to people, an organization, the air transportation system or national security as it relates to events such as 9/11. The intent of the definition is to focus on insider activity that could result in a catastrophic event for which TSA was created to prevent. There are other insider activities that could occur without causing such harm to the air transportation system. Those activities should be considered as indicators of vulnerabilities that could be exploited to harm the transportation system.

For the purpose of the insider threat definition under this task, the following is implied:

- The term "individuals" includes current or former employee(s), contractors or others who, whether on or off the airport, have/had access to sensitive areas and or information, or those who have developed insider knowledge through research or access to security sensitive tools, equipment, information or current or former employees.
- The term "sensitive" encompasses both physical space and information, whether on or off the airport, in comparison to the term "secure areas" which is limited to physical space.
- The term sensitive was chosen as an attribute to describe access to physical areas and information that require special protection, and/or are governed by legislation, regulation, policy, or other programs in order to prevent harm. Sensitive areas and information are restricted from the general public and protected from unauthorized access or disclosure respectively. The term sensitive extends beyond the TSA defined regulated areas which include Secured, SIDA, Sterile, and AOA to include physical space that may contain critical infrastructure, or other assets which warrant protection.
- "Intentionally or unwittingly" includes individuals with specific intent to use their access to cause harm, as well as those who utilize their access for an activity they did not realize could provide an opportunity for another individual to cause such harm.
- "Facilitate criminal activity…or other illicit actions" does not include petty crime such as theft or pilferage but rather criminal or illicit activity that would align with TSA's mission of protecting the nation's transportation system to ensure freedom of movement for people and commerce.
- Illicit actions may include criminal offenses, regulatory infractions, administrative rule or policy violations, or other unauthorized actions. Illicit is a term which is integral to the definition of insider threat because it is adaptable to a variety of insider schemes which may fall short of the elements of criminality or terrorism. Illicit actions may include conducting surveillance, gathering knowledge/intelligence to support criminal or terrorist activity, circumventing security, or violating the Known Crew Member Program. The term illicit is frequently referenced in policies and regulations including Title Code 21 of Federal

- Regulations Part 1301, Section 1301.92 Illicit activities by employees which references a position by DEA regarding employees, and Bank Secrecy Act (31 USC 5311-5330).
- A nexus with national security is established through the known grave consequences of catastrophic attacks on or through the aviation sector.

Definition

The following is offered as the definition of insider threat from an industry perspective, and is predicated on applicable points noted in the preamble above:

> *The term insider threat refers to 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.*

COMPARATIVE ANALYSIS OF LEADING DOMESTIC COMPANIES' INSIDER THREAT INITIATIVES

In the course of our research, it became clear that there are common fundamental elements to robust insider threat programs across domestic companies and aviation organizations. Previous work by Deloitte, the Intelligence and National Security Alliance (INSA) and the National Insider Threat Task Force, to specifically mention only a few, outlines the key considerations and fundamental elements to include as part of enterprise-wide insider threat programs.

Key considerations include:

- Define what insider threat means to your company or facility and identify the critical assets that your mitigation measures are aimed at protecting. Tailor the development of the program to address these specific needs, threat types, and your organization's unique culture. *One size does not fit all*.
- Leverage a broad set of internal and external stakeholders. Deloitte recommends that organizations establish cross-disciplinary insider threat working groups that can serve as change agents and ensure the proper level of buy-in across departments and stakeholders (e.g., legal, physical security, policy, IT security, human resources, ethics, etc.). *Support and involvement of senior leadership is key*.
- Awareness of observable behaviors that can serve as potential risk indicators for insider threat. According to the FBI's Insider Threat Program, detection of insider threat should use behavioral-based techniques. In addition, case studies analyzed by Carnegie Mellon University's Computer Emergency Response Team (CERT) program have shown that insider threats are rarely impulsive acts.
- Robust reporting structures for all stakeholders to report suspicious activity.
- Review personnel management practices and include regular audits to verify trust and related privileges granted to certain populations.
- Customized awareness and security training for all stakeholders throughout the company and organization.
- Formal and established insider threat response protocols and procedures.
- Constant reevaluation to maintain and adjust insider threat programs to industry trends, key risk indicators, and emerging and evolving threats.

The team analyzed the insider threat programs in place at various domestic companies and aviation organizations, including a major defense company, a U.S. air carrier and U.S. airports of all sizes. We approached each company with the following questions:

- How do you define insider threat in relation to your insider threat programs? What is the main focus? What are you trying to deter?
- How do you measure effectiveness of your programs?
- Please describe the size and scope of your company and size and scope of your insider threat program? What are the key elements of your program?

- Does the program incorporate a focus on external stakeholders such as third parties to include supply chain providers?
- What is the company's leadership support and involvement?
- What internal organizations (e.g., legal, HR, IT, security, law enforcement) are most involved in the program?
- What is the visibility and messaging put out to the company on the insider program?
- Please describe your insider threat training – if any – to your employees. Is training provided to any other external stakeholders?

Lockheed Martin

Members of the working group held a conference call with Mr. Douglas D. Thomas, Director, Counterintelligence Operations and Investigations and Ms. Kimberly O'Grady, Intelligence Analyst at Lockheed Martin. Lockheed Martin is a global security and aerospace company that employs approximately 100,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services.

The following was provided by Lockheed Martin as an explanation of its definition of Insider Threat, found at Appendix 1:

In November 2015, the Insider Threat Subcommittee, under the auspices of the Intelligence and National Security Alliance (INSA), and the Security Policy Reform Council (SPRC), undertook an initiative to review and refine the definition of Insider Threat with a goal of achieving broad consensus among the diverse base of constituents within INSA. The Subcommittee, comprised of representatives from the US Government and Industry noted three issues to be addressed:

1. There are several definitions in existence today promulgated by government, industry and professional associations.
2. Many of the definitions are not inclusive enough, failing to account for one or more aspects of threat posed by an insider.
3. Several industries are struggling with the threats posed by insiders and many articulated that the various definitions created barriers to efficient implementation of insider threat programs.

Through group discussion several proposals were made and subjected to critical peer review. The Subcommittee settled on the language that was briefed to the SPRC on December 4, 2015, who embraced the new definition. It was also briefed to the Director of Defense Security Service and the Director of the National Counterintelligence and Security Center, who both endorsed the inclusive nature of the definition and including language specific to instances of workplace violence. An explanation of the definition:

- The concise, yet inclusive nature of the definition was meant to relate to all industries and the US Government. Several definitions we reviewed are easily interpreted to only focus on

the US Government or the US Government and the Defense Industrial Base, to the exclusion of other industries such as Energy, Financial, Oil and Gas, Pharmaceutical, etc.

- The "threat" is a person as an "insider" is a human being.
- The reference to "authorized access" simply means the person has successfully gone through that agency's or that company's vetting process prior to a final hiring decision.
- "Access" refers to that person being granted the ability to become part of an organization, giving them access to facilities, other employees, information, networks, and other resources.
- "Wittingly or unwittingly" recognizes that the threat could have be done by a person purposefully, accidentally or through neglect.
- "Acts in contravention of law or policy", this requires that either a law or stated policy or practice was violated.
- "Harm through the loss or degradation" are really determined by that company or agency.
- The inclusion of language regarding "workplace violence" had everything to do with how "insider" was defined - a person who was granted access to people and facilities based on some form of vetting that resulted in a hiring decision.

Lockheed Martin uses a tool developed internally known as their risk analysis mitigation system to create behavioral and digital benchmarks for each of their over 100,000 employees.

In terms of measuring effectiveness of the program, Lockheed Martin referenced the challenge that airport operators, air carriers and TSA often face when asked to demonstrate the effectiveness of various security measures – it is impossible to prove a negative. Despite this challenge, Lockheed Martin reports a number of proactive metrics to its Board of Directors on an annual basis, including:

- Number of training and awareness sessions,
- Numbers of investigations,
- Number of files stopped from leaving the company,
- Activity reports from workplace violence and suicide prevention threat management teams, and,
- Investigative leads generated through the risk analysis mitigation system tool.

The fact that Lockheed Martin briefs its Board of Directors annually on insider threat mitigation is rare for a company of this size but demonstrates the importance of insider threat mitigation as an issue that is integral to the company's values. Prior to briefing the Board of Directors, the Counterintelligence Operations and Investigations team brief the CEO, COO and Executive Leadership Team throughout the year. There is a robust governance structure for the insider threat steering committee which includes CI, legal, human resources, corporate IT security, and ethics. The steering committee is responsible for the Concept of Operations that governs how the insider threat mission is executed.

Senior leadership is also part of the communications strategy to employees to explain why the program is important, who is involved and that there are watchers to watch the watchers. The program has partnered with the Lockheed Martin ethics hotline – an already popular and trusted tool within the organization. They also pair insider threat training with popular ethics training materials and courses.

Lockheed Martin could not overstate the importance of communications and training and awareness. In its communications, Lockheed Martin uses company-specific case studies to highlight that threats from insiders can (and do) happen at their company and that Lockheed Martin employees are potential targets for nefarious actors looking to infiltrate the company. The company also tailors its message and training to employees based on job roles. It uses different messaging media to appeal to different generations of employees – posters, e-mails, internal social media networks. Lockheed Martin also tailors the message to what employees may care most about – national security, their own financial security or their own physical security (workplace violence).

From across the airport operator community, the ASAC team surveyed a few domestic airports of varying sizes, and leveraged its own organic experience in airport operations. Findings were consistent with established and emerging standards to mitigate the Insider Threat, as found in security policy and recommendations. Recognizing that each airport must tailor its own security programs, recognized practices include:

- Employee training
- Employee awareness (See Something/Say Something) and recognition programs
- Recurrent vetting
- Badge audits – periodic and random
- Reduction of direct access points to an operational minimum
- Random screening throughout security restricted areas, and at other sensitive areas on and off the airport
- Two-factor badge authentication
- Use of biometrics in identity verification and access control
- Zoning security badges, to further limit employee access within restricted areas

The team noted that there is a list of effective measures compiled from airport vulnerability assessments available to airport operators. The list is posted on the Homeland Security Information Network, and includes a number of measures that mitigate the Insider Threat.

RECOGNIZED PRACTICES THAT ARE COMMON AMONG MATURE INSIDER THREAT PROGRAMS

Senior leadership support and involvement to focus on insider threat as a high risk across the enterprise.

Robust and continuous background check evaluations aimed at determining suitability and trustworthiness.

Create a culture of security awareness, including training and reward programs.

Advanced suspicious activity reporting programs based on continuous education and multiple reporting channels.

Restricting access to critical assets based on operational need.

Behavior-based employee monitoring, including ID and access control monitoring.

Investigative expertise to investigate situations of potential concern.

Engagement and partnership with law enforcement across multiple agencies to share information, increase available intelligence, and strengthen investigations.

Cross disciplinary working groups or consortia to meet regularly to share intelligence, review updated security policy and procedure changes, and any recent incidents whether international, national, regional or local.

Include insider threat related information in initial, on-going and recurrent training, stressing roles and responsibilities of all employees in mitigating insider threat.

Knowledge testing to reinforce training and security awareness and covert testing and auditing of security and required procedures.

INSIDER THREAT MITIGATION PROGRAMS AT INTERNATIONAL AIRPORTS

In conducting an analysis of international insider threat mitigation programs, the working group solicited specific information from various airports around the world. Given the sensitivity of the measures, relatively few airports responded, other than to provide very general information.

With limited details about insider threat mitigation programs at international airports and the short time frame for the initial report, there is an opportunity to conduct further analysis and in-country information exchanges at a later date.

However, most international airports adhere closely to the International Civil Aviation Organization (ICAO) security standards for Safeguarding International Civil Aviation Against Acts of Unlawful Interference.

In order to provide a means for comparative analysis, the working group attempted to assess mitigation measures in place at international airports in the same categories as identified by the ASAC Working Group on Airport Access Control:

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

Security Screening and Inspection

Although airports in Australia, Canada, Japan and New Zealand utilize physical screening as a major element of their insider threat mitigation programs, it is not "full" screening of aviation workers, nor is it used in isolation.[2] Instead, it is conducted on a random and continuous basis in conjunction with other security measures.

In accordance with a government mandate, airports in Japan implemented full physical screening of aviation workers. As a result, significant congestion occurred at various access control points, often interfering with airport operations and negatively impacting the flow of aviation workers. After a year, the government of Japan developed and ultimately transitioned to "multi-layered airport security measures," to enhance security and facilitate airport operations.

Through the multi-layered approach – that effectively involves the establishment of security perimeters, with aircraft being the last perimeter – airports in Japan placed more emphasis on enhanced access control points and focused the random physical screening of aviation workers on

[2] Given the aviation worker screening exemptions that exists for first responders, law enforcement, security personnel and others, the term "full" is used in lieu of 100 percent.

the identification of explosive materials. Security guards were stationed around aircraft to conduct observations in order to identify and detect unlawful interference. Aviation workers with access to aircraft may be subject to screening for "restricted carry-on items."

Airports in Europe rely primarily on full physical screening of aviation workers to mitigate the Insider Threat.

In Australia last year, the government announced its intention to enhance security at airports through the introduction of random aviation worker screening, tighter access controls and security awareness training. The Australian government directed a phased implementation of the enhanced security measures, and specifically designed them in a manner that provides "flexibility for airports to ensure they continue to function efficiently and effectively." Aviation workers at large airports in Australia along with their vehicles and accessible property are randomly selected for explosive trace detection testing and/or other screening methodologies when entering or working in security restricted areas.

In accordance with Transport Canada regulations, the Canadian aviation security system is based on an integrated, multi-layered approach involving security partnerships, intelligence sharing, risk assessments, policing, physical security, regulations, training and the use of physical processes, procedures and technology to mitigate risk.

Similar to the recommendation of the ASAC Working Group on Airport Access Control, which called for the development of a model to give all employees the expectation that they are subject to security screening/inspection at any time while working at an airport, aviation workers at Canadian airports must present themselves for screening prior to entering security restricted areas. The Canadian Air Transport Security Authority (CATSA) randomly subjects a percentage of aviation workers to physical screening procedures.

Rather than screening aviation workers for all prohibited items, many international airports have revised their screening measures to primarily focus on explosive materials.

Reportedly, a model similar to TSA's ATLAS model is being developed and rolled out at airports in Switzerland. The team was not able to fully explore this Swiss model, but ASAC will assess that model through the Insider Threat Subcommittee.

Background Checks and Vetting of Employees and Threat Assessments

In Australia, only aviation workers who have been subjected to and successfully passed a background check and an Australian Security Intelligence Organization security assessment are able to obtain an Aviation Security Identification Card (ASIC). The issuance of an ASIC may be refused if the background checks reveal certain criminal offenses, or revoked if criminal activity is subsequently discovered. However, airport operators determine and control the level of security restricted area access that is provided to ASIC holders.

Notably, two or more aviation-security-relevant offences, with no imprisonment, one of which was received within 12 months of the criminal history check, is sufficient grounds for denial of an ASIC.

In Canada, aviation workers whose duties necessitate access to security restricted areas at an airport must obtain transportation security clearance. Transport Canada verifies the suitability of each Transportation Security Clearance applicant with Citizenship and Immigration Canada, Royal Canadian Mounted Police and Canadian Security Intelligence Service. If Transport Canada obtains credible information indicating that an applicant or an existing pass holder poses a transportation security risk, the department refuses, suspends or revokes the clearance of the individual in question.

The holders of a transportation security clearance are perpetually vetted against criminal records to ensure there is no new derogatory information that would necessitate revocation of the clearance.

Upon successful completion of the transportation security clearance, the aviation worker may be issued a Restricted Area Identity Card (RAIC). The RAIC system, created by CATSA in partnership with Transport Canada and airport authorities, uses iris and fingerprint biometrics to limit access to security restricted areas of airports. The final authority responsible for granting access to security restricted areas of an airport is the airport operator.

It should be noted that many international airports lack the ability to perpetually vet aviation workers against both criminal and terrorism databases as is standard practice in the United States.

Internal Controls and Auditing of Airport-Issued Credentials

In accordance with European Commission regulation, to prevent the misuse of airport identification cards, a system shall be in place to reasonably ensure that attempted use of cards that have been lost, stolen or not returned is detected.

Security for Higher Risk Employee Populations and the Use of Intelligence

In Canada, Canadian Security Intelligence Service (CSIS) has district offices at some of the largest airports across the country. CSIS supports aviation security, and liaises with other departments and agencies with a presence at airports.

Security Awareness, Training and Vigilance

In Australia, security awareness training is required for aviation workers who regularly work in security restricted areas. The training is focused on enhancing the security culture and encouraging reporting of suspicious activity.

As stipulated in the Canadian Aviation Security Regulations, airports in Canada have established and implemented security awareness training programs that promote a culture of security vigilance and awareness among aviation workers. In order to obtain or renew their RAIC, aviation workers must take the training which may be delivered via classroom, video or computer-based formats.

In addition to a national Canadian Airport Security Awareness Program developed in coordination with the eight largest airports in Canada, some include airport-specific modules to impart additional information about their airport.

Of note, several high-level investigations that resulted in the arrest of aviation workers at airports in the United States can be attributed to security awareness training programs, such as the DHS "*If You See Something, Say Something*®" campaign. As emphasized during the training, vigilant aviation workers reported suspicious activity to the airport operator.

Appendix A: Insider Threat Definitions & Policy Scopes
(As of May 2018)

National Insider Threat Task Force (NITTF)

- *Executive Order 13587 (October 2011)*
  "ensure the responsible sharing and safeguarding of classified national security information"

- *National Insider Threat Policy & Minimum Standards (November 2012)*
  "Insider Threat means the threat that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities."

Department of Defense

- *National Defense Authorization Act (NDAA) For FY 17; Section 951 (2017)*
  "(3) The term "insider threat" means, with respect to the Department, a threat presented by the person who – (A) has, or once had, authorized access to information, a facility, a network, a person, or a resource of the Department and (B) witting or unwittingly, commits – (i) and act in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or (ii) a destructive act, which may include physical harm to another in the workplace."

- *DoD Instruction 5205.16 The DoD Insider Threat Program (Change 2 – August 2017)*
  "The threat insiders may pose to DoD and U.S. Government installations, facilities, personnel, missions, or resources. This threat can include damage to the United States through espionage, terrorism, unauthorized disclose of national security information, or through the loss or degradation of departmental resource or capabilities."

Department of Homeland Security

- *DHS Action Memorandum – Expanding the Scope of the DHS Insider Threat Program (December 2016)*
  "The threat that an insider will use his or her authorized access, wittingly or unwittingly, to d harm to the Department's mission, resources, personnel, facilities, information, equipment, networks, or systems. Insiders would include any person who has or who had authorized access to any DHS facilities, information, equipment, networks, or systems."

DSS & CLEARED INDUSTRY

- *NISPOM Conforming Change 2 (May 2016)*

"Insider Threat. The likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified national security information.

Carnegie Mellon University Computer Emergency Response Team (CMU CERT)

- *CMU CERT – Insider Threat Blog (March 2017)*
  "Insider Threat - the potential for an individual who has or had authorized access to an organization's assets to use their access, either maliciously or unintentionally, to act in a way that could negatively affect the organization."

Intelligence and National Security Alliance (INSA)

- The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.
- *INSA Website (September 2016)*
  "insider threats include the theft, loss, or leak of classified, sensitive, or proprietary information; the deliberate infliction of damage to an organization's facilities, operations, or networks; or violence or harassment perpetrated by a trusted insider against other employees of the organization, whether at the workplace, at another location, or online;"

TSA

- *TSA Management Directive No. 2800.17 Insider Threat Program (July 2013)*
  "Insider Threat: One or more individuals with access and/or insider knowledge that allows them to exploit vulnerabilities of the Nation's transportation systems with intent to cause harm. This includes direct risks associated with TSA's security programs and operations, as well as the indirect risks that may compromise our critical infrastructure. For purposes of the TSA Insider Threat Program, insiders are, or present themselves to be, current or former transportation sector employees, contractors, or partners who have or have had authorized access to transportation sector facilities, operations, systems, and information."

  Note: TSA's definition is derived, in part, from a President's National Infrastructure Advisory Council (NIAC) report dated April 2008. The NIAC developed a working definition for the insider threat to critical infrastructures. The NIAC applied and tested this definition throughout the Study, and the definition helped shape policy recommendations for addressing the insider threat. The following is the outcome of the Study's development and testing process for a definition of insider threat to critical infrastructures:

The insider threat to critical infrastructure is one or more individuals with the access and/or inside knowledge of a company, organization, or enterprise that would allow them to exploit the vulnerabilities of that entity's security, systems, services, products, or facilities with the intent to cause harm.

In deliberations on the definition of the insider threat, the NIAC carefully considered the importance of *access* – access to the systems, facilities, or information where an infrastructure's vulnerabilities lie. Inclusion of all people with access expands the group of potential insiders beyond company employees, to include unescorted vendors, consultants, and contractors with access to an infrastructure's facility or IT system.

U.K. Centre for the Protection of National Infrastructure (CPNI)

- *CPNI INSIDER DATA COLLECTION STUDY (April 2013)*
  "an insider is defined as a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes."

Analytic Exchange Program (AEP) (Public-Private Partnership sponsored by DHS and ODNI)

- *AEP Aviation Insider Threat Team Report (2017)*
  Page seven of this report contains several public-private definitions the study team collected during their research to include:
  - US Airline: According to a US Airline, the insider threat is a current or former employee, contractor, vendor, or other business partner, who has or had authorized access to an organization's information, abilities, products, or supply chain. This knowledge or access is then misused to negatively affect the organization or to do harm to the public.
  - Private Sector Company: According to a private sector company, insiders are persons who have the potential to harm an organization for which they have inside knowledge or access. An insider threat can have a negative impact on any aspect of an organization, including employee and/or public safety, reputation, operations, finances, national security and mission continuity.
  - TSA: TSA defines insider threat as an individual with the intent to cause harm and with access and/or insider knowledge that would allow the individual to exploit vulnerabilities of the nation's transportation systems. In the aviation domain, this potentially includes current or former TSA employees and contractors, airline employees, cleaning and catering crews, construction and maintenance workers, law enforcement, military and security forces, taxi cab drivers or transportation specialists, or other airport personnel who have access and/or insider knowledge.
  - FBI: "'Insiders,' which are corrupt employees who exploit their credentials, access, and knowledge of security procedures."

National Institute of Standards and Technology (NIST) – Three definitions found at https://csrc.nist.gov/Glossary/?term=4852

- CNSSI 4009-2015 (Adapted from CNSSD No. 504)
  The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities. (This definition closely aligns with the definition under NITTF)

- NIST SP 800-53 Rev. 4 (CNSSI 4009)
  An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.

- NIST SP 800-53 Rev. 4 (Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs)
  The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.

Lockheed Martin

- The threat presented by a person who has, or once had, authorized access to information, facilities, networks, people, or resources; and who wittingly, or unwittingly, commits: acts in contravention of law or policy that resulted in, or might result in, harm through the loss or degradation of government or company information, resources, or capabilities; or destructive acts, to include physical harm to others in the workplace.

- Lockheed Martin shared the following explanation which provides an insightful frame of reference to understand the context of their definition.
  - The concise, yet inclusive nature of the definition was meant to relate to all industries and the US Government. Several definitions we reviewed are easily interpreted to only focus on the US Government or the US Government and the Defense Industrial Base, to the exclusion of other industries such as Energy, Financial, Oil and Gas, Pharmaceutical, etc.
  - The "threat" is a person, a human being as an "insider"
  - The reference to "authorized access" simply means the person has successfully gone through that agency's or that company's vetting process prior to a final hiring decision

- "Access" refers to that person being granted the ability to become part of an organization, giving them access to facilities, other employees, information, networks, and other resources
- "Wittingly or unwittingly" recognizes that the threat could have be done by a person purposefully, accidentally or through neglect
- "Acts in contravention of law or policy", this requires that either a law or stated policy or practice was violated
- "Harm through the loss or degradation" are really determined by that company or agency
- The inclusion of language regarding "workplace violence" had everything to with how "insider" was defined - a person who was granted access to people and facilities based on some form of vetting that resulted in a hiring decision

Note: This definition was included in the most recent National Defense Authorization Act and it has been endorsed by the Director of National Intelligence (DNI) and Department of Defense (DOD).

Massport

- A insider threat is anyone with privileged access to sensitive areas, information and/or assets that an organization values most, who misuses this access, either wittingly or unwittingly, to facilitate criminal activity, terrorist activity, or illicit actions which inflict harm to an organization or national security.

Federal Aviation Administration

- Any employee who uses their granted privileges or access to harm personnel, facilities, networks, or information (wittingly or unwittingly) is an Insider Threat. The Unwitting Insider is defined as a trusted employee or contractor who, without malice, causes harm to the organization. (FAA)

Other Definitions (multiple sources)

- **Insider threat** is a malicious **threat** to an organization that comes from people within the organization: employees, former employees, contractors, vendors, etc. who have inside information – knowledge, information, and access, regarding an organization's security practices, data and systems that can be exploited for malicious reasons ranging from criminality and personal gain – e.g. economic espionage, theft, furtherance of terrorism/ideology, and ultimately to inflict violence.

- A t**hreat** from people within the organization such as current or former employee's, contractors, vendors etc. who have inside information, knowledge, and access, regarding an organization's security practices, data and systems that can be exploited for malicious

reasons ranging from criminality and personal gain e.g. economic espionage, theft, furtherance of terrorism/ideology, and ultimately to inflict violence.

- Any risk posed by a current or formerly trusted individual with access or privileged knowledge; used to damage, deprive, diminish, injure or interrupt organizational stakeholders, assets, critical processes, information, systems or brand reputation. Insider threats include any illegal, prohibited or unauthorized conduct (acts or omissions).

Appendix B: Members of ASAC Working Group on Insider Threat at Airports

Steve Alterman
President
Cargo Airline Association

Paul Arnold
Director, Aviation Security
United Parcel Service

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

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

Scott Broyles
President and CEO
National Safe Skies Alliance

Frank Capello
Director of Security, Broward County Aviation Department
Fort Lauderdale-Hollywood International Airport

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

Michele Freadman
Deputy Director, Aviation Security Operations
Massachusetts Port Authority

Randy Harrison
Vice President, Corporate Security
Delta Air Lines

Jens Hennig
Vice President, Operations
General Aviation Manufacturers Association
Stephen Holl
Chief of Police (retired)
Metropolitan Washington Airports Authority Police Department
Airport Law Enforcement Agencies Network

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

Janulyn Lennon
Director of Security
Hartsfield-Jackson Atlanta International Airport

Craig Lowe
Director of Security Operations
Airlines for America

John McGraw
Director, Regulatory Affairs
National Air Transportation Association

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

Gary Wade
Vice President Security
Atlas Airlines

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

Transportation Security Administration (Adjunct Members)
Serge Potapov, Tamika McCree, Dan McCann