OFFICE of PRIVATE SECTOR

SLICKSHEET

OVERVIEW OF INSIDER THREATS TO AVIATION IN 2020

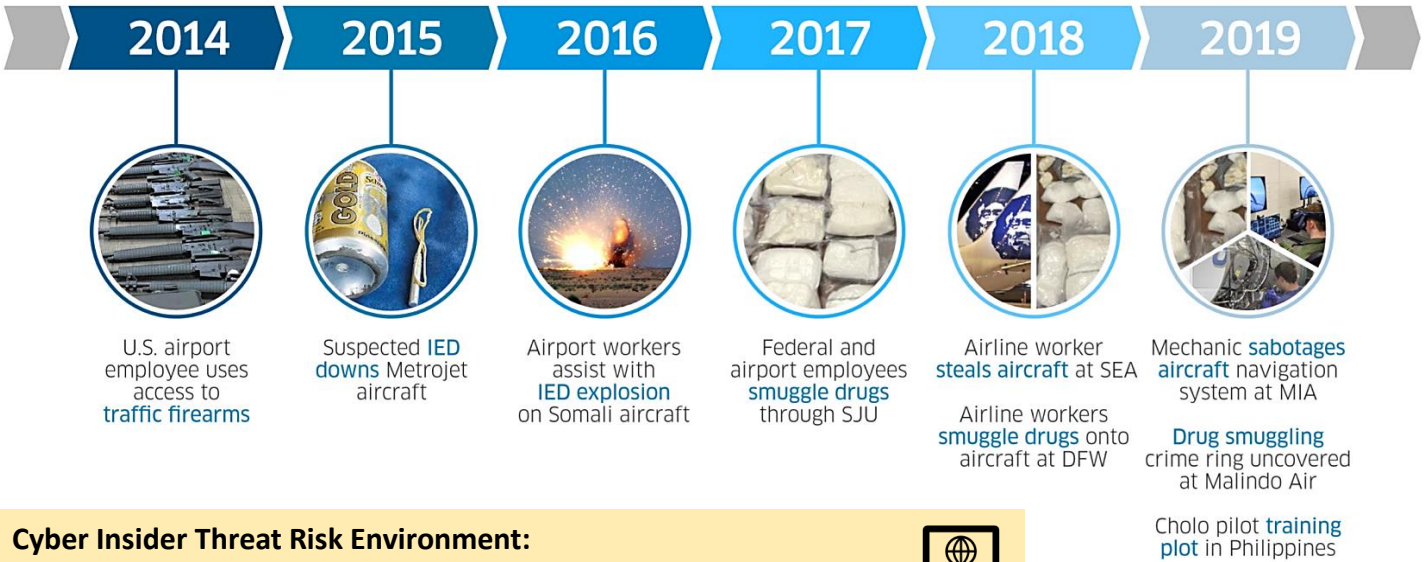
On 10 September 2020, the FBI's Los Angeles Field Office and InfraGard hosted a virtual meeting for private sector and government partners to address ongoing insider threats to the aviation industry.

What is an Insider Threat?

TSA defines Insider Threat as the threat that an individual with authorized access to sensitive areas and/or information will wittingly or unwittingly misuse or allow others to misuse this access in an effort to exploit vulnerabilities to compromise security, facilitate criminal activity, terrorism, or other illicit actions that inflict harm to people, organizations, the transportation system, or national security (*2020 TSA Insider Threat Roadmap*). The FBI considers the Insider Threat as one of the most pressing concerns for aviation security. Terrorists are known to monitor aviation security and have an interest in manipulating airport and airline employees to facilitate their operations, both as a conduit for exploiting vulnerabilities and to circumvent airport security countermeasures (*FBI LIR 191113006*).

Insider threats can take many forms and manifest in a variety of ways, including:

- Terrorism or extremist activities
- Sabotage
- Subversion
- Smuggling of persons or contraband
- Corruption, to include participation in transnational organized crime
- Attempted or actual espionage
- Unauthorized access to security restricted areas and information
- Unauthorized disclosure of information
- Conspiracy to commit a criminal offense
- Workplace violence



Cyber Insider Threat Risk Environment:

- Cyberattacks affecting the aviation ecosystem
- Current or terminated employees installing malware
- Current or terminated employees stealing proprietary or sensitive information
- Terminated employees accessing systems that control the aviation ecosystem

TLP:GREEN

Detect, Deter, and Mitigate Insider Threats

"An insider who has to overcome multiple security layers to carry out an attack is more likely to be pre-empted, deterred, or defeated during the attempt. Efforts to counter insider threats require collaboration among TSA, federal partners, law enforcement, state and local authorities, and industry stakeholders, including transportation workers" - 2020 TSA Insider Threat Roadmap

Detect – Indicators and Suspicious Activities

- Seeking opportunities to work alone and/or unsupervised shifts
- Monitoring personnel or vehicles entering/leaving facilities or parking areas
- Discreetly using cameras, video recorders, binoculars, or note taking and sketching
- Acting nervous or exhibiting secretive behavior, sweating, avoiding eye contact with police/security
- Enthusiastic interest in security matters outside the scope of duties
- Avoiding or attempting to block security cameras
- Placing objects in sensitive or vulnerable areas to observe security responses
- Misusing credentials
- Making threatening comments of violence against the United States or individuals (*FBI LIR 191113006*)
- Accessing restricted areas outside the performance of official duties/access control violations alone or with unauthorized visitors
- Disregard for security policies/procedures; repeated violations

Deter

- Require valid ID from all employees and visitors; do not allow "piggybacking" to badge in
- Be aware of people and actions that are suspicious (e.g., asking probing security/operational questions)
- Develop and expand incident reporting requirements
- Implement network and access controls
- Conduct vulnerability assessments from the Insider Threat perspective
- Audit and monitor existing security policies and processes
- Adjust tactics often on security posture so as not to allow threat actors to circumvent security procedures

Mitigate

- Maintain employment and dismissal records — Report all dismissals and separations to credentialing office promptly
- Use Rapback and Air Domain Computer Information Comparison programs
- Provide additional training and engagement with employees as part of the security culture and as front-line eyes and ears to see any potential security risks
- Encourage awareness (See something/Say something)
- Conduct random badge/ID media audits, including use audits
- Implement recurrent vetting
- Conduct random and unpredictable screening within and at security restricted area (SRA) access points, prioritizing measures to counter the threat of improvised explosive devices and coordination with the Advanced Threat Local Allocation Strategy screening program
- Utilize multi-factor employee authentication
- Review and refine access privileges and access points to the SRAs (including Security Identification Display Areas/Air Operations Area)

If you have questions or requests for support, FBI Aviation Liaison Agents (ALAs), TSA Assistant Federal Security Directors-Law Enforcement (AFSD-LEs), TSA AFSDs for Inspection (AFSD-Is), and TSA Field Intelligence Officers (FIOs) are ready and able to assist. The ALAs respond to incidents at airports, conduct interviews, coordinate actions such as secondary screenings, assist in vulnerability assessments, and provide trainings as a part of the FBI's counterterrorism mission. AFSDs-LE are the primary TSA law enforcement officials in the airport and are involved with insider threat mitigation, outreach, and awareness in coordination with the TSA Insider Threat Program and local stakeholders. AFSD-Is ensure regulatory compliance and play a key role in identifying and mitigating vulnerabilities.

TSA Contact Information: **TSA.I&A.FIID.Management@tsa.dhs.gov**

To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx. For more information on TSA's Insider Threat Program, please contact: 1-855-257-6919, or insiderthreat@tsa.dhs.gov. If you have questions or requests for TSA I&A support from your local Field Intelligence Officer, please email TSA.I&A.FIID.Management@tsa.dhs.gov.

This Slicksheet was disseminated from the OPS Information Sharing and Analysis Unit and prepared in collaboration with the Los Angeles Field Office, InfraGard, the NJTTF Civil Aviation Security Program (CASP), and the U.S. Transportation Security Administration. Direct any requests and questions to the FBI Private Sector Coordinator or ALA at your local FBI Field Office: https://www.fbi.gov/contact-us/field-offices.