International Civil Aviation Organization
ICAO South American Regional Office
Fourteenth Meeting of the Civil Aviation Authorities of the SAM Region (RAAC/14)
(Santiago, Chile, 27, 28 and 30 October 2015)

Agenda Item 3: Review of results obtained in the SAM Region on security matters

INSIDER RISK IN CIVIL AVIATION

(Presented by the United States)

SUMMARY

Insiders may exist within nearly every organization, including civil aviation authorities. Recognizing the various risks, drivers, and motivations of an insider can aid in mitigating insider risk. In becoming more aware of insider risk, civil aviation organizations and other appropriate authorities can strengthen security in direct support of International Civil Aviation Organization Annex 17, Chapter 4.

Action:
Recommendations are being provided in Paragraph 4

***ICAO Strategic Objectives*:**	*Security and Facilitation*

1. Introduction

1.1 In December 2013, an airport employee with extensive knowledge of the security measures at a Wichita, Kansas airport intended to detonate a vehicle full of explosives on the tarmac. The airport employee had studied the layout, flight patterns, and passenger volume and was radicalized through activity on the internet via *Inspire*, a publication by al-Qaeda in the Arabian Peninsula. An alleged drug smuggling ring was uncovered at a New Orleans, Louisiana airport that operated from October 2013 through June 2014. Airline records detail how seven packages were shipped to the airport through airline cargo and, in other cases, investigators say drug traffickers personally carried narcotics in passenger luggage and handed the luggage over to airline employees in the airport's bathroom. These examples can be defined as insiders—a security screener, employee, vendor, or contractor at an airport, able to use his/her trusted position, knowledge, and access to commit a malicious, complacent, or ignorant act.

1.2 An insider is not restricted to a specific group or person and can result from a multitude of motivators. Personal factors that can motivate an individual can range from ideology, greed/financial need, anger/revenge, the thrill, and/or vulnerability to blackmail. Expanding on the initial example, an insider can include airport employees, contractors, government agency employees, construction/maintenance crews, cleaning crews, vendors, security screening personnel, law enforcement, baggage handlers, aircraft mechanics, ticketing agents, and taxi/limousine drivers.

1.3 The Transportation Security Administration (TSA) has sought to raise awareness of insider risk and has implemented significant efforts to educate stakeholders on how to mitigate insider risk. TSA has focused on providing workshops on insider risk at various domestic and international locations to identify, evaluate, and mitigate insider risk.

2. Insider Risk

2.1 There are many risks that insiders pose to an airport due to their unique access to areas that are otherwise restricted. The prevalence of insider risk is based upon possible insider threats, which include:

- **Espionage** is the use of insider access to obtain sensitive information for exploitation that impacts national security.
- **Security compromise** is the use of access to override or circumvent security countermeasures like drug and contraband smuggling.
- **Sabotage** is the intentional destruction of equipment or material.
- **Workplace violence** is the use of violence or threats that cause a risk to the health and safety of the workforce and traveling public.
- **Terrorism** is the use of access to commit or facilitate an act of violence as a means of disruption or coercion for political purposes.
- **Physical property theft** is the use of insider access to steal material items, including passenger possessions or equipment.
- **Information theft** is the use of insider access to steal or exploit information.

2.2 Insider risk is a combination of vulnerability and insider threat; however, they are not interchangeable terms. Vulnerability is when there are gaps in a system that an insider could exploit, e.g. no background checks, poor access control, etc. Insider threat is when someone has the intent or capability to do something, which is then elaborated with the three attributes of insiders.

2.3 The three primary attributes of insiders that may result in insider risk are ignorance, complacency, and malice. Ignorance occurs when there is a lack of awareness of policies and procedures that creates risk. This is particularly prevalent when dealing with emerging threats or new employees. Personnel using social media may fit into the category of ignorant insider by providing valuable information to the public that can be exploited to conduct an attack. Complacency occurs with an employee’s negligent approach to policies, procedures, and potential security risks. Complacent insiders often assume that specific behaviour does not have a noticeable impact and that no one is monitoring their behaviour. In this instance, the complacent insider does not perceive their behaviour as having an impact on the organization and may have a careless approach to potential security risks.

2.4 Malicious insiders are those who actually intend to cause harm and typically develop a plan in advance. Malicious insiders are typically motivated by a limited number of factors such as money, ideology, and/or revenge. By conducting a malicious act, they intend to benefit financially, materially, or to simply prove a point, inflict harm or correct a perceived injustice. Malicious insiders can be susceptible to coercion, especially if a personal circumstance makes them vulnerable. An example could be a worker in severe financial difficulties that is targeted by an outside entity that wants insider access to an airport. Another example could be an airport employee that is targeted by an outsider through the use of blackmail with the intent to use that employee’s insider status to commit a malicious act.

2.5 There may be several behavioural indicators associated with malicious insiders. It is important to recognize potential signs, which may include previous violations of the law or history of social or mental health problems. Other more subtle indicators may include routine tardiness, procedural violations, and/or interpersonal conflicts with colleagues. It is also important to be aware of potential factors outside of work that exert stress on employees such as financial, personal, or legal problems.

2.6 Countermeasures are essential to reducing insider risk and can include people, process, and/or technology that help to mitigate the threat. Increasing security awareness and holding employees accountable to procedures are essential to risk mitigation. Access control, policies, procedures, training, and initial and recurring background checks are part of a layered approach to help in mitigating all types of insider risk. The United States utilizes a layered approach with background checks, perpetual vetting, and the use of random and unpredictable security measures. This is in line with Annex 17 Standards and Recommended Practices that outline the importance of background checks and the selection process for employees, as well as the use of screening and other security controls.

3. Conclusion

3.1 An insider - a security screener, employee, vendor, or contractor at an airport - is able to use his/her trusted position and access to commit a malicious, complacent, or ignorant act. Their privileged access and knowledge of vulnerabilities allow for a higher likelihood of success if policies and procedures are not in place to mitigate this risk. In order to understand how to mitigate insider risk, it is critical to understand how an insider can obtain access with the intention to cause harm. Insider risk has the potential to exist within every organization, and it is critical to recognize the various risks, drivers, and motivations of an insider. Raising awareness and sharing best practices will better enable States to more adequately and effectively address vulnerabilities and mitigate the insider risk.

4. Suggested action

4.1 The Meeting is invited to:

a) Acknowledge that insider risk is an issue that civil aviation organizations must address, and encourage States within the region to share best practices in mitigating this risk.

- END -