International Civil Aviation Organization

WORKING PAPER

A39-WP/180
EX/67
10/08/16

ASSEMBLY — 39TH SESSION

EXECUTIVE COMMITTEE

Agenda Item 16: Aviation Security – Policy

GLOBAL STRATEGIES FOR ADDRESSING INSIDER RISK

(Presented by the United States)

EXECUTIVE SUMMARY

The International Civil Aviation Organization (ICAO) and its Contracting States have traditionally focused on identifying externally-facing threats to the civil aviation environment. However, aviation systems remain vulnerable to the risks posed by insiders, which exist in nearly every industry, including civil aviation. Efforts by civil aviation organizations and other appropriate authorities to recognize, understand, and implement appropriate actions to address insider risks can strengthen security in direct support of ICAO Annex 17 – *Security*, Chapter 4. The United States remains committed to addressing these issues through information sharing and best practices exchange.

Action: The Assembly is invited to:

a) acknowledge that insider risk is an issue that every civil aviation organization must address, and encourage States to share best practices in mitigating this risk through the appropriate ICAO and regional forums. Greater understanding of the scope and potential consequences of this issue requires additional cross-disciplinary consideration and discussion on this subject across ICAO working bodies, independent initiatives, and other aviation security forums;

b) agree that this concept should be reflected in documentation outlining ICAO's strategic priorities for the next triennium, as well as the Global Aviation Security Plan (GASeP), in order to ensure that resources are properly devoted to strengthening global capacity to address insider threats;

c) consider whether tools outlined in this paper can be used to support current ICAO and Contracting State initiatives to include the development of insider risk training materials. ICAO Regional Offices should take an active role through the sharing of locally developed inputs and the dissemination of new products to regional communities; and

d) direct ICAO Aviation Security Panel bodies to review current information on insider threat and risk within ICAO Annex 17, as well as the guidance contained in Sections 11.2 and 11.3 within Chapter 11 of the Aviation Security Manual – Doc 8973.

Strategic Objectives:	This working paper relates to the Strategic Objective C – *Security and Facilitation.*
Financial implications:	This paper has no significant financial implications.
References:	None

1. INTRODUCTION

1.1 Over the past triennium, ICAO and its Contracting States have enhanced capabilities to mitigate ever-evolving external risks to the aviation security environment through increased collaboration. Although significant progress has been made to address external risks, the global community must remain mindful that risk does not solely originate from the peripheral boundaries of each civil aviation system. The world is operating in a threat environment that is dynamic, rapidly evolving, and increasingly reliant on insiders to facilitate new attacks. According to the 2016 ICAO *Risk Context Statement*, "Terrorists continue to view insiders as a useful resource to facilitate attack planning, either knowingly or unknowingly, because of their specialized knowledge of security measures and potential access to security restricted areas and aircraft." Due to their unique access to areas and/or information that are otherwise restricted, trusted individuals may pose many risks to the airport and to the aviation system as a whole.

1.2 While mainstream security measures are designed to restrict the public's access to secure facilities within the airport, these controls may not sufficiently mitigate insider risks. Over the past several years, numerous incidents have highlighted how the value of security controls intended to prevent external attacks are significantly reduced or negated when insiders with the knowledge and capability exploit these security controls. As a result of these concerns, the United States recognizes that this threat cannot be overlooked or underestimated and, as such, the global community must focus more attention on understanding and managing these risks.

1.3 Although considerable progress has been made to better define and understand the scope of this subject, it is critical that all aviation security stakeholders continue this momentum through the development and deployment of tailored solutions. In order to build an aviation security infrastructure that can withstand both internal and external threats, the United States encourages the exchange of best practices and tools that can better equip the entire aviation network to manage the threat. As part of its commitment to this effort, this paper discusses recent efforts within the United States to implement solutions, as well as ongoing work to improve current capabilities.

2. DISCUSSION

2.1 Historically, ICAO and Contracting States have prioritized resources to control access to sensitive areas of the airport's operations from external threats. However, these measures may not adequately address airport personnel currently operating within secure areas. Staff categories can include: aircrew, maintenance personnel, baggage handlers, security guards, and janitorial staff. These individuals are considered insiders since they are able to use their trusted and verified position and access to commit negligently or deliberately destructive acts against civil aviation.

2.2 Over the past several years, the world has witnessed incidents when trusted insiders played a critical role in breaches of security and the perpetration of acts of unlawful interference and other illicit activity within the civil aviation domain. These acts may vary from espionage to sabotage or full-scale acts of terrorism because insiders have access to areas restricted to the public and may use this privileged access to conduct these acts. For example, while the installation of new screening equipment may ensure that the travelling public are appropriately screened, security screeners trained in the use of this equipment can exploit its vulnerabilities to defeat its purpose. It is absolutely critical that Contracting States understand these issues and recognize that traditional countermeasures may not effectively address the insider threat.

2.3 ICAO and its Member States have supported a number of recent efforts to better understand the scope of the insider risk and understand these unique vulnerabilities; these efforts have resulted in new tools and guidance material on the subject. Most notably, Contracting States are advised to first conduct a risk assessment to identify threat scenarios pertinent to their location and associated vulnerabilities to determine appropriate countermeasures for implementation. Careful consideration should be paid to ensure that countermeasures are effective against identified threat scenarios while leveraging international best practices and guidance such as intelligence-based employee background checks and the random, unpredictable deployment of countermeasures.

2.4 Like many of its partners, the U.S. Transportation Security Administration (TSA) actively strives to understand and better manage insider risk. As part of its risk-based approach to security, TSA continuously reviews the vulnerabilities to the aviation system, evaluates the performance of current countermeasures intended to mitigate risks, and identifies both new and existing tools that can be optimized to ensure a more robust security system. These solutions are implemented in an intelligence-driven, risk-based manner using random and unpredictable measures. The solutions are implemented by a flexible and highly-trained workforce with the aid of advanced, cutting-edge technology combined with the proactive engagement of relevant stakeholders and the travelling public in the security process.

2.5 To bolster the security measures that are employed across the U.S. civil aviation network, TSA has invested in the creation and cultivation of a robust security culture – an organizational philosophy that encourages optimal security performance. TSA has implemented risk-based security as a key initiative underpinning the overall transportation security culture within the United States. For TSA, effective risk management considers how to provide the most effective security in the most efficient way to fulfill our counterterrorism mission and protect the traveling public. Risk management is not a no-risk approach; it includes multiple and overlapping elements of security at airports, ongoing vulnerability assessments, and a concerted quality control program. In addition to these key features, open lines of communication and raising awareness of all invested government entities and commercial partners are imperative to enhance attention toward security risks.

2.6 TSA relies on multiple methods of security to protect the traveling public and safeguard the nation’s transportation system from both internal and external threats. Although checkpoint operations are often considered the most visible element of security, they represent only one of many components that make up TSA’s security architecture. TSA has implemented additional security measures to reduce insider vulnerabilities, including policies and procedures designed to ensure a secure environment. TSA has established an Insider Threat Program to introduce an element of unpredictability into security operations by varying where, when, and how security resources are employed beyond the baseline measures implemented at all times. The intent is to complicate, lengthen, and deter terrorist planning efforts. As part of TSA’s commitment to multiple methods to address security, it has implemented countermeasures such as access controls, employee lifecycle management, training and awareness, and policies and procedures.

2.7 While mitigating actions may vary, countermeasures can build on each other to form a layered approach to reducing risk in an effective and efficient manner. TSA has bolstered its capabilities across four categories:

a) Access Controls: These include many of the security measures designed to prevent unauthorized personnel from accessing secure or restricted areas.

b) Employee Lifecycle Management: By establishing a continuous personnel management process, which begins with the initial hiring to continuous and recurrent

vetting through to final termination, organizations can proactively maintain a secure workforce.

c) Training and Awareness: Periodic security training that includes insider threat awareness supports a stable culture of security within an organization. Without broad understanding and buy-in from the entire workforce, current countermeasures become less effective.

d) Policies and Procedures: In order to strengthen the use of these protocols, countermeasure requirements should be integrated and enforced through a unified security policy.

2.8 In February 2016, the TSA Administrator addressed the 207th ICAO Council and committed to sharing the U.S. experiences and efforts to identify proactive measures that bolster security. As part of this process, TSA has undertaken efforts to create a new enhanced training program designed to educate employees on the current threat picture to the aviation environment, equip recipients with the critical thinking skills to identify and recognize atypical behaviors, and enable them to articulate and report concerns. Through conceptualization and planned release of this training, TSA seeks to increase security domain awareness so that individuals are empowered to detect, deter, and report potential or actual security threats throughout the aviation network.

2.9 Domain awareness training will be tailored to the recipient's work environment. The course will enable employees to assess applicable threats to their domains and, through a series of exercises, accomplish the following objectives: train them to identify potential attack methods and correlating suspicious behavior, establish an effective response, and proactively report concerns to the appropriate persons. By improving the vigilance of an entire workforce, this tool is expected to expand countermeasure coverage across the entire airport and create an additional element of security to reduce both internal and external vulnerabilities.

3. CONCLUSION

3.1 ICAO and its Contracting States can play a critical role in ensuring that the aviation community is better equipped to understand and manage the scope of insider-facilitated attacks against the network. To supplement the global response to an ever-evolving threat, the United States encourages its partners to share best practices through information sharing, the exchange of successful tools and other guidelines, and the promotion of greater cross-collaboration on this subject. Accordingly, the United States remains committed to sharing its tools and training products with ICAO and Contracting States. The dissemination of these products is the first step toward strengthening the global aviation security network. The exchange of solutions that promote insider awareness by empowering an entire workforce to serve as the eyes and ears of the aviation system can serve as an additional, forward-leaning, and innovative resource for the prevention of future insider attacks.

— END —