International Civil Aviation Organization

**WORKING PAPER**

## SECOND HIGH-LEVEL CONFERENCE ON AVIATION SECURITY (HLCAS/2)

**Montréal, 29 to 30 November 2018**

**Agenda Item 1: Aviation security threat and risk context**

# INSIDER THREAT AND SECURITY CULTURE

(Presented by Austria on behalf of the European Union and its Member States[1], the other Member States of the European Civil Aviation Conference[2])

**SUMMARY**

Insider threat presents one of the most serious and growing concerns for aviation security, and it shall be addressed without undue delay. An effective global response to insider threat is essential to the sustainable success of the GASeP and to ensure that aviation security objectives more generally are not undermined. It is best dealt with through a combination of robust and consistently implemented regulatory measures, and through the development and promotion of security culture for all employees/contractors working in or for the air transport sector.

Action by the High-level Conference on Aviation Security is in paragraph 4.

## 1. INTRODUCTION

1.1 Terrorists consistently look to exploit vulnerabilities in security controls in an attempt to find the path of least resistance to their targets. This could mean the exploitation of people in the form of employees/contractors working in or for the aviation sector whose role provides them with privileged access to secured locations, secured items or aviation security information. By exploiting these individuals with privileged access, they can gain a potential tactical advantage in perpetrating or facilitating an act of unlawful interference. The personnel that may be so exploited includes flight crew and all ground-based employees in airports or other facilities related to air transport and its supply chains and encompasses contract, temporary or self-employed personnel as well as full- or part-time staff members.

1.2 Insider threat can also take the form of ill-intentioned persons having interest in obtaining employment in the aviation sector at large with the intent of having this tactical advantage for the perpetration of an act of unlawful interference or contributing to it. Or, over the course of time, existing

[1] Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and United Kingdom.

[2] Albania, Armenia, Azerbaijan, Bosnia and Herzegovina, Georgia, Iceland, Republic of Moldova, Monaco, Montenegro, Norway, San Marino, Serbia, Switzerland, The former Yugoslav Republic of Macedonia, Turkey and Ukraine.

employees/contractors may become radicalised with an intent to assist with or attempt an act of unlawful interference. The on-going increase in trends such as unprecedented speed under which radicalisation (and self-radicalisation) can occur has been confirmed by the ICAO Working Group on Threats and Risk.

1.3 How to address the insider threat already in the pre-employment phase before an individual is hired/contracted, throughout the employment relationship and even after the termination shall be reflected by the employer's processes i.e. background check, vetting, active promotion of a healthy security culture.

1.4 Insiders have been involved in a number of attacks and attempted attacks on aviation. In particular, it appears certain that there was insider involvement in the introduction and explosion of improvised explosive devices on Metrojet flight 9268 in October 2015 and Daallo Airlines flight 159 in February 2016. At a lower level, of risk directly to flight, there are numerous examples of individuals using insider access and the absence of effective controls to exploit security vulnerabilities for other purposes such as smuggling of drugs or the unauthorised carriage of firearms. Therefore, an effective global approach to insider threat is essential to ensure that the overall security concept is not undermined.

1.5 Moreover, dealing with insider threat is also essential to the successful implementation and sustainability of the Global Aviation Security Plan (GASeP). The GASeP contains as priority action 1.7.1G to *"Review adequacy of current measures to address insider threat, including background checks, physical measures, training and awareness and reporting mechanisms."* Clearly, the benefit from the enhanced security performance that we expect from the GASeP could be undermined if security measures leave a gap in the form of a vulnerability posed by an "insider".

## 2. REGULATORY MEASURES TO DEAL WITH INSIDER THREAT

2.1 To address the vulnerability posed by insider threat demands a multi-layered approach, as no single measure itself can deliver a sufficiently high level of protection. The essential, and complementary, components in this multi-layered approach should be as follows:

- Access control for all persons other than passengers and for vehicles;

- 100% screening of persons other than passengers and the items they carry on entry into secure areas;

- A comprehensive system of security controls for vehicles, airport and in-flight supplies;

- Randomness and unpredictability built into that screening and/or within secure areas;

- A comprehensive employment process that includes an understanding of each function, the access to secure areas or sensitive information that necessarily comes with those functions ("need to know" principle), and the potential risks thus created; and

- A system of background checks on all personnel with unescorted access to and working in secure areas and enhanced checks (e.g. security vetting) on personnel with access to sensitive parts of the aviation operation and/or sensitive information, including those implementing security measures.

2.2 It is important that all six of these components are in place. A system of 100% screening that contains no randomness and unpredictability is insufficiently effective as insiders wishing to defeat security can learn about a predictable system through being exposed to it regularly and may be able to identify and exploit vulnerabilities in it. Equally, systems of background checks that do not involve 100% screening will not stop the use of "clean skin" insiders (those with no criminal history or known terrorist connections), nor people who are subject to coercion, are giving unwitting assistance to terrorists, have been radicalised rapidly or who have undiagnosed mental issues. Understanding of the necessary insider access associated with certain functions enables additional measures to be applied to those areas of greatest risk. Furthermore, access control measures complement these measures and assist the manageability of security processes by limiting the staff in secure areas to those with a clear operational need.

2.3 Europe is committed to tackling insider threat and underscores the importance of addressing it globally. It stands ready to cooperate with all international partners in efforts and initiatives to effectively mitigate the insider threat. [3]

## 3. SECURITY CULTURE

3.1 Beyond regulatory requirements it will be of even greater longer-term importance to ensure that responses to insider threat are part of a positive security culture. Its development supports and complements security requirements, while adapting to an ever evolving threat landscape. It also highlights the importance of investment in human resources, which in turn brings improvements in the way security requirements are implemented in practice.

3.2 Security culture is included as the second Priority Action in the GASeP, which sets out that:

> *"The promotion of effective security culture is critical to achieve good security outcomes. A strong security culture must be developed from the top management across and within every organization. The existence of a well-trained, motivated and professional work force is a critical prerequisite for effective aviation security."*

3.3 An effective security culture means that all relevant government and industry workforce, from senior management to the employees, and indeed members of the public, are engaged with and take responsibility for security issues. It means that those lapses in security that can happen from time to time are dealt with or drawn attention to immediately by colleagues, rather than allowing an unsatisfactory situation or practice to persist in a way that it could become a vulnerability capable of being exploited by terrorists. It can reduce the likelihood of security breaches occurring in the first place, as staff develops the habit of thinking and acting in more security-conscious ways. It can also have a beneficial effect on morale if it is promoted in a manner that emphasises that a healthy security culture is about supporting each other's efforts to create a secure industry rather than being "watched" on by others. Therefore, every element of the airport network (and beyond) has to be security aware and empowered. By creating a strong security culture we are reducing risks/vulnerabilities.

3.4 While there is broad consensus on the importance of the promotion of security culture, practical actions to deliver this objective have so far been relatively limited. It is important that States,

[3] For a description of actions undertaken by the European Union and its Member States to address Insider Threat see WP-45 as presented to the 2018 AVSECP/29. For a description of the vulnerability assessments on insider threats undertaken by the European Civil Aviation Conference see WP/43 presented to the 2018 AVSECP/29.

industry and training organisations use the wide range of guidance material and tools available to support the implementation of strong security culture behaviours within organizations, including training materials and awareness and behaviour change campaigns to ensure that this consensus is translated into action on the ground.

3.5 It is likely that aviation security actors can learn from the experience of aviation safety in this respect. Safety improvements have been made in the past as a result of persistent and highly visible campaigns run over long periods to drive home clear messages. Aviation campaigns related to foreign object debris are one such example. The aims of the GASeP in relation to security culture require changes to day-to-day activity that will take some time to become normalised. But they can deliver great benefits, in particular in relation to tackling insider threat, in ensuring that aviation sector employees are all contributing to a high quality of security performance generally; and in particular are helping, through their vigilance and security awareness, to thwart activities of insiders who seek to use their position to commit or assist acts of unlawful interference. In time, we should hope that this high level of security awareness would become one of the most important protections against insider threats.

## 4. ACTION BY THE HIGH-LEVEL CONFERENCE

4.1 The High-level Conference on Aviation Security is invited to:

a) Reaffirm the importance of measures to deal with insider threat and urge the ICAO Council, based on advice of its Aviation Security Panel, to enhance Standards and Recommended Practices in Annex 17 to deal with insider threat based on all components of the multi-layered approach presented in this paper;

b) Urge States and industry to ensure the effective implementation of regulatory measures regarding insider threat, as these measures are key to ensure that other measures are not undermined by a compromise of the system through insiders; and

c) Urge States and industry to promote security culture as a means of addressing insider threat, through initial and recurrent training and through high-profile campaigns aimed at the aviation workforce and the public to raise their awareness.

— END —