



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

**Montréal, 29 to 30 November 2018**

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

**UPDATE ON AVIATION SECURITY THREAT AND RISK**

(Presented by the Secretariat)

**SUMMARY**

The various attacks to civil aviation infrastructure across the globe, along with the continuous intent and growing capability of terrorist groups to exploit vulnerabilities in the system, prove that international civil aviation remains a prime target for a variety of motives. As such groups and individuals develop new techniques and weapons to circumvent and/or defeat security systems and processes, States must remain vigilant and keep under constant review the level and nature of threat to civil aviation within their territory and airspace above it, as required by Annex 17 — *Security*.

Action by the High-level Conference on Aviation Security is in paragraph 5.

**1. INTRODUCTION**

1.1 Identifying, understanding and addressing the potential risks to international civil aviation is paramount to building a global, robust aviation security system that is sustainable in the face of the continuing threat of terrorism. Following the first High-level Conference on Aviation Security (HLCAS/1, Montréal, 12-14 September 2012), an outcome-focused and risk-based approach to aviation security was recognized as the best way to address the evolving threats to international civil aviation on a global scale. Consequently, the ICAO Global Risk Context Statement (RCS), developed and maintained in collaboration with the Aviation Security (AVSEC) Panel's Working Group on Threat and Risk (WGTR), was deemed a useful tool for developing evidence-based risk assessments and identifying possible mitigating actions that States may implement to achieve risk-based security programmes.

1.2 As risks vary from region to region, identifying gaps and addressing vulnerabilities in aviation security systems remain a challenge that requires strong international cooperation among all actors, including States, industry stakeholders and relevant national agencies. Supported by United Nations (UN) Security Council resolution 2309 (2016): *Threats to international peace and security caused by terrorist acts: Aviation security*, which urged that all States cooperate to safeguard aviation against terrorist attacks, ICAO is committed to ensure that international security standards are reviewed, updated, adapted and implemented based on current risks, while anticipating the evolution of the threat picture.

## 2. CURRENT MAJOR RISKS TO INTERNATIONAL CIVIL AVIATION

### *Improvised explosive devices*

2.1 As evidenced by the restrictions placed on the carriage of portable electronic devices (PEDs) by some States, improvised explosive devices (IEDs) remain the weapon of choice in attempts to attack civil aviation and airport infrastructure. The overall threat posed by IEDs concealed in personal items, including PEDs, represents a serious concern. In addition, other forms of concealment, including in hold baggage and cargo consignments, have re-emerged as areas of growing concern, as terrorist groups continue to show intent and capability in that regard, and are always seeking vulnerabilities and new and diverse ways to defeat aviation security systems. This could result in the exploitation of people (e.g. airport employees) or processes (e.g. ineffective security measures) that may allow a terrorist to use less sophisticated weapons to conduct an attack.

### *Chemical, biological and radiological threat*

2.2 The assessed risk posed by the use of chemical, biological and radiological (CBR) agents has increased, following a disrupted plot in July 2017 to take an IED on board an aircraft and the subsequent discovery by Australian authorities of attempts to construct an improvised chemical dispersion device designed to release highly toxic hydrogen sulfide, which would cause mass fatalities in a confined space. In this regard, it is critical that States, international organizations and industry share with ICAO any information on viable and effective measures capable of mitigating the CBR threat, to facilitate the development of a global and harmonized framework of mitigation measures – an approach that proved to be successful in addressing the liquids, aerosols and gels (LAGs) issue in 2006.

### *Evolution of the threat*

2.3 With centralized attack planning, terrorist groups have the ability to leverage resources and skills to pursue sophisticated tactics against relatively hardened targets. However, as the planning of attacks becomes more decentralized, there is an expansion of tactics, techniques, and procedures to less sophisticated weapons targeting more vulnerable and easily accessed targets, such as the public areas of airport terminals. It should be noted that following the recent attacks to the landside of airports (Belgium on 22 March 2016, Turkey on 28 June 2016, and the United States on 6 January 2017), ICAO strengthened Annex 17 provisions on the matter as part of Amendment 15 to Annex 17 (Standards 4.8.1, 4.8.2, and 4.8.3 refers).

2.4 Through the radicalization of individuals across the globe, the threat to civil aviation has expanded into areas of the world that may not have previously experienced such attacks. In effect, terrorist groups continue to demonstrate the capability to devise and inspire attacks across a broad geographical area, including through the recruitment of foreign fighters. As the area of active conflict continues to evolve, foreign terrorist fighters may be repositioned to carry out attacks anywhere, including in their home States.

2.5 While there is evidence of intent by terrorist organizations to use cyber means to commit acts of terrorism that could endanger civil aviation, no cyber-attacks qualified as catastrophic or endangering aviation safety have occurred to date. However, the potential threat posed by such attacks on civil aviation through air traffic management, aircraft or airport systems continues to be a source of concern. On 24 October 2017, a State Computer Emergency Response Team (CERT) requested transport networks to be on alert as a new wave of cyber-attacks took place, one of which hit a major international airport and the capital's metro system. The attack caused some flight delays. Such occurrences are a reminder that the aviation community should remain vigilant and protect their critical information and

communication technology systems and data from unlawful interference, as required by Annex 17 Standard 4.9.1.

### **3. COMBATING INSIDER THREAT**

3.1 The threat posed by insiders and the exploitation of airport staff continues to represent a real concern as terrorist groups are reported to actively look for insiders to assist in their attempts to target civil aviation. It is further heightened by the radicalization of individuals in many parts of the world, thus reducing the opportunities for their detection by conventional vetting methods, by people close to them, or by security or law enforcement services. For example, on 25 October 2017, a pilot working for the Bangladesh national carrier was arrested on suspicion of terrorism, including plotting to keep passengers hostage and flying a commercial plane into the houses of top government leaders. The 31-year old Boeing 737 pilot was reported as having close links with a terrorist group.

3.2 The integrity of security checkpoints is undermined when staff can circumvent a checkpoint without being subject to screening and security controls (Annex 17 Standard 4.2.6 refers). Failure to address the insider threat could result in a displacement of the IED threat and greatly undermine mitigation efforts. Daallo Airlines flight 159 from Somalia to Djibouti, on 2 February 2016, was a prime reminder of the seriousness of the threat; it has been determined that the modified laptop computer, causing a hole in the fuselage, was made possible through the assistance of screening personnel.

3.3 As almost any form of attack could potentially include scenarios with an insider component, it is critical that States comply with Annex 17 Standards and Recommended Practices and take initiatives to assess the specific risks posed by insiders to their systems and organizations. In that regard, the subject of insider threat should be addressed within the context of proposals for a future Amendment 17 to Annex 17 by strengthening the related provisions, in order to mitigate the associated risks as soon as possible.

### **4. EFFECTIVE SHARING OF INFORMATION**

4.1 Sharing appropriate and relevant aviation intelligence information on new threats, and implementing effective mechanisms to exchange such information, are essential to facilitate the development of coordinated counter-measures to protect civil aviation. The 2010 Declaration on Aviation Security, ICAO General Assembly Resolution A39-18 *Consolidated statement of continuing ICAO policies related to aviation security*, the ICAO Global Aviation Security Plan (GASeP) and United Nations Security Council resolution 2309 all call for strengthened cooperation and information-sharing among States and with stakeholders concerned.

4.2 In keeping with the above, and particularly GASeP's Priority Outcome 1, *Enhance Risk Awareness and Response*, States and industry alike are encouraged to implement mechanisms to help make informed decisions on efficiently and effectively addressing new and emerging threats, and to avoid unilateral and/or uncoordinated implementation of security measures. In this respect, the three principles of cooperation in aviation security, recommended by HLCAS/1 and enshrined in ICAO Resolution A39 - 18, should be considered before imposing unilateral aviation security measures on States and industry partners without prior engagement and consultation with the State(s) concerned. To that end, stronger cooperation between States, specifically in the sharing of information between appropriate aviation security authorities, is needed. Accordingly, bilateral agreements or model clauses for the reciprocal sharing of information should be developed and used. UN Resolution 2309 further supports those principles by calling States to "engage in dialogue on aviation security and cooperate by

sharing information, to the extent possible, about threats, risks, and vulnerabilities, by collaborating on specific measures to address them and by facilitating, on a bilateral basis, mutual assurance about the security of flights between their territories.”

4.3 In light of the critical need for comprehensive collaboration and information-sharing, Amendment 16 to Annex 17 introduced a new Standard 3.1.4 that requires States to establish and implement procedures to share, as appropriate, with its airport operators, aircraft operators, air traffic service providers or other entities concerned, in a practical and timely manner, relevant information to assist them to conduct effective security risk assessments relating to their operations. Recognizing the challenges in developing or adapting legislation to enable information sharing mechanisms, States should ensure that the necessary legal and practical measures are in place to facilitate the timely exchange of threat and risk information, especially when operationally critical.

## 5. ACTION BY THE HIGH-LEVEL CONFERENCE

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

- a) remind States of the current threat to aviation while recognizing the importance of progressive aviation security enhancement;
- b) urge States to continue to refer to the ICAO Risk Context Statement (RCS), while recognizing the importance of adapting it to the unique situation of each State and region, as appropriate;
- c) recognize the importance of comprehensively addressing the insider threat through the processing of Amendment 17 to Annex 17 at the earliest opportunity; and
- d) recommend the need for a global framework for better threat information sharing.

— END —