55th CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGIONS

Denarau Island, Nadi, Fiji
22 — 26 October 2018

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

ENHANCING AVIATION SECURITY THROUGH CLOSER COLLABORATION AND ADOPTION OF A RISK-BASED APPROACH

Presented by the International Air Transport Association (IATA)

INFORMATION PAPER

SUMMARY

Ensuring security while sustaining traffic growth requires greater collaboration among all stakeholders and adoption of a risk-based approach to aviation security to ensure that capabilities and resources are utilized to maximum effect. This paper highlights the importance for all stakeholders including States to consider a risk-based approach to aviation security and benefits of enhancing collaboration in this domain.

ENHANCING AVIATION SECURITY THROUGH CLOSER COLLABORATION AND ADOPTION OF A RISK-BASED APPROACH

1. INTRODUCTION

1.1 Given the forecast growth in air travel and continuously evolving threat landscape, security risks should be assessed and mitigated through a systematic process. Today's aviation security measures work, but at great cost to airlines, airports, authorities, and to passengers. Adding new measures or the simple replacement of old equipment with new is not enough to ensure robust security. IATA believes a risk-based and outcome-focused approach can result in enhancing security through collaboration (including consultation and information sharing) among different stakeholders.

1.2 Leveraging on the ICAO Annex 19 on Safety Management System (SMS), IATA Operational Safety Audit (IOSA) Program imposes Security Management System (SeMS) on IOSA airlines. Also, ICAO Annex 17 Standard 3.1.3, the ICAO Global Aviation Security Plan incorporates key aspects of UNSCR 2309 (2016) and ICAO Assembly Resolution A39-18, reiterating the need for an effective, sustainable and risk-based implementation of security measures that are assessed regularly to reflect the evolving threat picture.

1.3 Risk management is a fundamental component of the SeMS framework underpinning all other security processes as described in IATA SeMS Manual. SeMS is an organized, systematic approach to managing security by embedding security management into the day to day activities of an organization. It provides the necessary organizational structure, accountabilities, policies and procedures to ensure effective oversight. In summary, a SeMS is an assurance system for security.

1.4 The SeMS Manual provides guidance on implementing efficient, accurate and cost managed controls and thus enhances a company's security culture, regulatory collaboration and resource utilization. The SeMS Manual also provides guidelines on building effective aviation security measures and supports a proactive, strategic and risk-based approach to protective security focusing on outcomes.

1.5 Another important element of enhancing global aviation security is closer collaboration and consultation with the industry, including information sharing. While IATA recognizes that aviation security is the primary responsibility of States and that industry must grant deference to the needs of appropriate authorities to act promptly when confronted with an immediate security threat or vulnerability, IATA also believes that it is the effective partnership between government of the State and industry that has made the air transport system the safest and most secure form of long-distance travel today. IATA calls on States for direct consultation with industry to ensure effective risk-based measures are implemented via multiple options instead of a single prescriptive measure.

2. DISCUSSION

2.1 To manage risks in a timely, effective and proportionate fashion, an assessment is needed of the threat, vulnerability and mitigation variables to estimate the level of 'residual risk'. The aviation industry faces the challenge of balancing all these variables in order to maximize the use of limited time and resources including personnel and funding.

2.2 Risk initially stems from the result of a threat–real or perceived–and is a combination of two factors:

2.2.1 intent—the desire someone may have to mount an attack; and
2.2.2 capability—their ability to commit the act they wish to undertake.

2.3 The threat, when combined with vulnerability, coupled with unanticipated or expected consequences that may result should a successful attack occur equates to risk. Having accounted for existing mitigation, the element of risk that remains is known as the 'residual risk'. While little can be done by individual entities to directly reduce any given threat (the intent and capability of potential perpetrators), reducing vulnerabilities or increasing mitigation activity will contribute to a reduction in risk and thus potentially minimize the consequence of such an attack on operations.

2.4 In effect, the goal should be to ensure that capabilities and resources are utilized to maximum effect, while at the same time seeking to prioritize activities in a proportionate, sustainable and carefully considered manner. Organizations which base their decision-making on risk-based, outcome-focused approach assess identified risks to decide on priorities followed by risk treatment actions fitting individual risk thresholds and also engage resources in the most efficient manner. Such an approach includes periodic review and adjustments.

2.5 Selecting the most appropriate risk treatment option involves balancing the costs and efforts needed for implementation as well as legal, regulatory and other requirements against the benefits derived. In doing so, where possible, the root causes of the risk must be treated, and the mitigating actions and controls tailored to the cause.

2.6 To avoid security measures being introduced without sufficient consideration to other consequences (for example impact on safety procedures) an impact assessment should typically be compiled. Such an assessment should provide evidence that measures have been assessed for its necessity and proportionality and associated risks have been considered.

2.7 The use of advanced security technologies and innovative methods/concepts towards implementing effective, risk-based and efficient levels of security should be promoted and fast tracked. This is especially relevant when considering the forecasted traffic increases, in particular from source regions perceived to be exposed to higher levels of threat. Though any substantial change of procedures should allow sufficient lead time for planning and implementation.

2.8 IATA fully supports effective implementation of the Annex 17 Standards 3.1.3 by States and recognizes the positive role of the national aviation security committees as described in Annex 17 3.1.5. These are mechanisms enabling the industry to actively participate and provide input for new/ amended legislation and/or measures with equal benefit for regulators.

2.9 However, regulatory responses to security risk are often based on unilateral decisions. To develop security measures that effectively counter threats to aviation, government of the State are urged to work in partnership with airlines, airports and other aviation security stakeholders.

2.10 A consultation process should happen before new measures are introduced wherein industry's feedback and views are taken into account prior to the introduction or revision of the existing measures. Industry input is critical and the collaboration between the key aviation stakeholders will benefit the planning process and ensure better outcomes.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to:

a) note the value of risk-based approach and collaboration in aviation security; and

b) note the importance of risk management methodology (for example as described in IATA Security Management System Manual)

— END —