International Civil Aviation Organization

The Sixth Meeting of the APANPIRG ATM Sub-Group (ATM/SG/6)

Hong Kong, China, 30 July – 03 August 2018

Agenda Item 9: Any other business

AIR TRAFFIC MANAGEMENT SECURITY REQUIREMENTS

(Presented by ICAO Asia and Pacific Office – Security)

SUMMARY

This paper presents information on Air Navigation Service Providers (ANSP) and Air Traffic Management Security Requirements and additional information relating to the establishment of cyber security guidance material and resources.

This paper needs updating to include developments in the past 12 months and to have more focus on implementation issues (and solutions).

1. INTRODUCTION

1.1 Aviation security SARPs are contained in Annex 17 - *Security* and have relevance to many other Annexes including, but not limited to, Annex 2, 6, 8, 9, 10, 11, 14 and 18. There are also connections with PANS Docs 4444 and 8168.

1.2 Annex 17 – *Security* requires States to develop and implement a National Civil Aviation Security Programme (NCASP), which should specify the roles and responsibilities of all the organizations and agencies, including Air Traffic Services (ATS) Providers, that may be involved in security operations. The NCASP addresses the whole range of security activities including, *inter alia*, threat and risk assessment, staff selection and training (in security-related matters), access control and other preventive security measures, management of response to acts of unlawful interference, and quality control.

1.3 Not all provisions of the NCASP will be applicable to the ANS Providers. The NCASP identifies the specific responsibilities of each of the parties that have a role in security operations.

2. DISCUSSION

2.1 There are a number of Standards and Recommended Practices (SARPs) with particular relevance to ATS Providers and ATM security contained in the 10 Edition (Amendment 15) of Annex 17 – *Security* (applicable as of 3 August 2017) including primarily Standard 3.5 but also to varying degrees, a number of additional SARPs with direct relevance as follows;

- ***3.5 Air traffic service providers***

Each Contracting State shall require air traffic service providers operating in that State to establish and implement appropriate security provisions to meet the requirements of the national civil aviation security programme of that State.

- ***4.2 Measures relating to access control***

4.2.2 Each Contracting State shall ensure that security restricted areas are established at each airport serving civil aviation designated by the State based upon a security risk assessment carried out by the relevant national authorities.

4.2.3 Each Contracting State shall ensure that identification systems are established in respect of persons and vehicles in order to prevent unauthorized access to airside areas and security restricted areas. Identity shall be verified at designated checkpoints before access is allowed to airside areas and security restricted areas.

4.2.4 Each Contracting State shall ensure that background checks are conducted on persons other than passengers granted unescorted access to security restricted areas of the airport prior to granting access to security restricted areas.

- ***4.8 Measures relating to the landside***

4.8.1 Each Contracting State shall ensure that landside areas are identified.

4.8.2 Each Contracting State shall ensure that security measures are established for landside areas to mitigate the risk of and to prevent possible acts of unlawful interference in accordance with risk assessments carried out by the relevant authorities.

4.8.3 Each Contracting State shall ensure coordination of landside security measures in accordance with Standard 3.1.5, 3.2.2 and 3.2.3 between relevant departments, agencies, other organizations of the State, and other entities, and identify appropriate responsibilities for landside security in its national civil aviation security programme.

- ***4.9 Measures relating to cyber threats***

4.9.1 ***Recommendation****.— Each Contracting State should, in accordance with the risk assessment carried out by its relevant national authorities, ensure that measures are developed in order to protect the confidentiality, integrity and availability of critical information and communications technology systems and data used for civil aviation purposes from interference that may jeopardize the safety of civil aviation.*

4.9.2 ***Recommendation****.— Each Contracting State should encourage entities involved with or responsible for the implementation of various aspects of the national civil aviation security programme to identify their critical information and communications technology systems and data, including threats and vulnerabilities thereto, and develop and implement protective measures to include, inter alia, security by design, supply chain security, network separation, and remote access control, as appropriate.*

- **5.2 Management of Response to Acts of Unlawful Interference**

5.2.2 Each Contracting State responsible for providing air traffic services for an aircraft, which is the subject of an act of unlawful interference, shall collect all pertinent information on the flight of that aircraft and transmit that information to all other States responsible for the air traffic services units concerned, including those at the airport of known or presumed destination, so that timely and appropriate safeguarding action may be taken en-route and at the aircraft's known, likely or possible destination.

5.2.3 Each Contracting State shall provide assistance to an aircraft subjected to an act of unlawful seizure, including the provision of navigation aids, air traffic services and permission to land as may be necessitated by the circumstances.

5.2.4 Each Contracting State shall take measures, as it may find practicable, to ensure that an aircraft subjected to an act of unlawful seizure which has landed in its territory is detained on the ground unless its departure is necessitated by the overriding duty to protect human life. However, these measures need to recognize the grave hazard attending further flight. States shall also recognize the importance of consultations, wherever practicable, between the State where that aircraft has landed and the State of the Operator of the aircraft, and notification by the State where the aircraft has landed to the States of assumed or stated destination.

5.2.6 ***Recommendation.—*** *Each Contracting State should ensure that information received as a consequence of action taken in accordance with 5.2.2 is distributed locally to the air traffic services units concerned, the appropriate airport administrations, the operator and others concerned as soon as practicable.*

2.2 States' compliance with the above mentioned SARPs are subject to auditing under the ICAO Universal Security Audit Programme - Continuous Monitoring Approach (USAP-CMA).

2.3 A new Amendment 16 to Annex 17 – *Security* has been approved by the ICAO Council with an effective date 16 July 2018, and applicable date 16 November 2018. Amendment 16 contains several new provisions that have a bearing on Air Traffic Management Security Requirements in addition to those already established in the current Amendment 15 to the Annex.

3.1 National organization and appropriate authority

New *Standard 3.1.3 bis Each Contracting State shall 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.*

4.9 Measures relating to cyber threats

New *Standard 4.9.1 Each Contracting State shall ensure that operators or entities as defined in the national civil aviation security programme or other relevant national documentation identify their critical information and communications technology systems and data used for civil aviation purposes and, in accordance with a risk assessment, develop and implement, as appropriate, measures to protect them from unlawful interference.*

Amended Recommended Practice 4.9.2 Each Contracting State shall ensure that the measures implemented protect, as appropriate, the confidentiality, integrity and availability of the identified critical systems and/or data. The measures shall include,

inter alia, security by design, supply chain security, network separation, and the protection and/or limitation of any remote access capabilities, as appropriate and in accordance with risk assessment carried out by its relevant national authorities.

5.1 Prevention

New *Standard 5.1.6* *Each Contracting State shall ensure that its civil aviation security programme defines processes for the reporting of information concerning incident of acts of unlawful interference and preparatory thereto, by any entity responsible for the implementation of the national civil aviation security programme and in a practical and timely manner for the relevant authorities, as appropriate, taking into account 2.1.4*

(**Recommended Practice 2.1.4 — Each Contracting State should ensure appropriate protection of aviation security information*)

2.4 In accordance with its leadership role, and in recognition of the vital role played by ATSPs and the security of ATM, ICAO has drafted guidance to assist States to establish and implement the appropriate security provisions as required by the relevant SARPs which would include the physical and electronic protection of all relevant facilities and equipment. The Air Traffic Management Security Manual (Doc 9985) is available to States for convenience. This Manual complements the *Aviation Security Manual* (Doc 8973 – Restricted) and provides guidance on security issues specific to ATM in order to assist States and ATS Providers in implementing appropriate security provisions to meet the published requirements of the NCASP. In addition, the manual provides guidance to the ATS Providers on provision of ATM security services in support of national security and law enforcement requirements, and guidance on protection of the ATM system infrastructure from threats and vulnerabilities.

2.5 The 10th Edition of the ICAO Aviation Security Manual (Doc 8973) incorporates new guidance material relating to cyber security developed in accordance with the European Civil Aviation Conference (ECAC). The ICAO global Risk Context Statement (RCS) is updated annually. The latest version 7 was endorsed by the AVSECP/29 and will soon be available. The RCS provides a methodological approach to Risk assessment (including ATM/cyber risks) – to support States in developing their national threat/risk evaluation/mitigation system. The current 6th Edition of the global RCS defines the risk of cyber security attacks against civil aviation as low. However, this is in a global risk context and assessed in regard to all potential forms of acts of unlawful interference with civil aviation. The risk level may vary based on individual States own risk assessments and/or risk assessments conducted by relevant agencies for their own operations.

2.6 ICAO has established a secure repository of cybersecurity-related guidance material https://portal.icao.int/cybersecurity. A public repository for cyber security-related material is available at https://www.icao.int/cybersecurity/Pages/default.aspx

2.7 Furthermore, ICAO has established an Industry High-level Group (IHLG) Civil Aviation Cybersecurity Action Plan – signed 5 December 2014. The Action Plan established clear timeframes for the achievement of goals and targets to facilitate the development of a common understanding of cyber threats and risks, and mechanisms needed to promptly share and communicate related information between government and industry stakeholders.

2.8 Development of an ICAO global ATM/cyber security training is on the way based on existing EUROCONTROL material and in cooperation with EUROCONTROL. EUROCONTROL has already developed an ATM security training package and continues on its further development.

2.9 An ICAO Europe, Middle East and Africa (EMEA) Cybersecurity in Civil Aviation Summit was conducted in Bucharest, Romania 7 to 9 May 2018. The summit concluded with the publication of the Bucharest Communique, containing six recommendations for ICAO's cybersecurity strategy.

2.10 The Third Meeting of the ICAO Secretariat Study Group on Cybersecurity (SSGC) was conducted from on 9 and 10 May 2018 in Bucharest. Work carried out by the SSGC to proactively address cybersecurity issues continues to develop a cybersecurity framework.

2.11 With input from India, Malaysia, Hong Kong, Indonesia and Singapore including both ATS and AvSec professionals, the Cooperative Aviation Security Programme-Asia Pacific (CASP-AP), has drafted the following.

- Text to be inserted into the CASP-AP Model National Civil Aviation Security Programme (NCASP) outlining the requirements as per Standard 3.5 and the other relevant SARPs and security practices and mechanisms; and
- A CASP-AP National Air Traffic Service Provider Security Programme (CASP-AP ATS Security Programme) model/template. The model/template addresses the preservation of the ATM system and the use of the ATM system in the response to acts of unlawful interference.

2.12 The appropriate text has been included in the latest version of the CASP-AP Model NCASP released to CASP-AP member States/Administrations. The draft CASP-AP ATS Programme is available to Member States and will be released also to non-CASP-AP States on request.

2.13 States are encouraged to share information and best practice regarding their effort to comply with Annex 17 – *Security* Standard 3.5. An example includes sharing of ATS Providers Security Programs.

3. ACTION BY THE MEETING

3.1 The meeting is invited to:

a) note the information contained in this paper;

b) make use of the relevant available guidance material and resources;

c) ensure regulatory compliance with the International and National requirements for ATS Providers and ATM Security; and

d) encourage States that already have security provisions in place for air traffic service providers to share information with other States.

…….