In cooperation with

ICAO

CANSO

AIRBUS

LATIN AMERICA & THE CARIBBEAN

AIR TRAFFIC MANAGEMENT CYBERSECURITY POLICY TEMPLATE

SHAPING OUR FUTURE SKIES

canso.org

Acknowledgements

This document was produced by the International Civil Aviation Organization (ICAO), Civil Air Navigation Services Organisation (CANSO) and Airbus.

The following individuals are recognised for their valuable contributions:

- **Mayda Ávila**, Regional Officer, Communications, Navigation and Surveillance, ICAO NACC Office
- **Julien Touzeau**, Product Security Director, Americas, Safety, Security & Technical Affairs – AAG, Airbus
- **Yann Berger**, Product Security Expert, APSYS – Product Security, Airbus
- **Gaelle Hubert**, Governance specialist and security auditor, Airbus
- **Poulin Estelle**, Physical security specialist, Aviation Security specialist and ACC3 auditor, Airbus
- **Javier Vanegas,** Director, Latin America and Caribbean Affairs, CANSO
- **Shayne Campbell**, Safety Programme Manager, CANSO
- **Eduardo Garcia**, Manager European ATM Coordination and Safety, CANSO

Contents

Introduction

The first decade of the twenty-first century has seen an increase in terrorist activity against a range of targets using a variety of methods. These have ranged from the use of explosive devices in attacks against aircraft, trains, and buildings, to cyber-attacks against information and communications systems. At the same time, systems and equipment supporting air navigation services have evolved towards digitalization and connectivity making them vulnerable to cyber–attacks. Information management systems supporting real-time decision-making are sensitive and deserve special protection attention.

Cyber-attacks are becoming a growing threat worldwide as a result of increased digitalization and the interconnectivity of systems. Civil aviation is particularly sensitive to this emerging threat due to its widely interconnected systems. Any disruption of systems due to a cyber-attack can seriously impact the safety and security of flights and also the reputation of civil aviation in the public eye. As such, ICAO addressed this emerging threat to civil aviation through resolution A39-19 "addressing cybersecurity in civil aviation" during the 39th Assembly.

It is vital that the civil aviation sector integrates cybersecurity policies as part of their normal procedures, and integrates them in every part of their aviation system.

Within this context, Air Traffic management (ATM), Communication, Navigation and Surveillances system (CNS), Information Management (IM) and other important systems for aviation are exposed to many different types of potential risks, arising from:

- Actions that may be intentional and hostile,
- Accidental or negligent,
- Impact from natural disaster.

Aeronautical systems are vulnerable to cyber threats such as IT sabotage, data corruption and availability (notably ransomware), software corruption, communication disruption or interruption, satellite communication interference, cyber-attacks including systems sabotage, data breaches, damage and destruction of hardware. Cyber threats can also be part of a bigger plot to harm people such as kidnapping, hostage taking, physical injuries and death.

Civil Aviation Authorities and Air Navigation Services Providers in the Latin America and Caribbean Region are concerned about the increased threat of cyber attacks stemming from the implementation of state-of-the-art technology without the necessary protections and resilience procedures to ensure they continue to meet the agreed levels of safety. It is recommended, therefore, that States broaden their cybersecurity vision to encompass air navigation systems, taking into account satellite systems (e.g. ADS-B), information systems, air traffic management systems and others that may be vulnerable to cyber-attacks. Digitalization and Internet connectivity mean that previously non-suspicious equipment is now vulnerable.

In order to protect their operation from internal and external threats, States should implement cybersecurity mechanisms across the entire ATM system.

It is also recommended that cybersecurity be included in the security culture through the training of air transport personnel (Air navigation services provider [ANSP], airlines and airports). The application of good basic practices introduced in training can reduce the probability of cyber-attacks which, although representing a minimal risk to security, can affect public confidence.

While new technologies may be better prepared to resist cyber-attack, the legacy technologies that are still in use at airports, airlines and ANSPs may not be as prepared. As a result, cybersecurity is considered as an interrelated matter by ICAO because of its functions and inter-connected technology. The reason for this is the perceived threat of a cyber-attack affecting aerodrome operations, airworthiness and air navigation systems and services.

1. How to use this document

This document does not replace any national regulation.

States, in accordance with their Aeronautical Technical/Operational Infrastructure, should:

- Identify critical infrastructures related to communications, navigation and surveillance of air traffic services and protect them accordingly.
- Protect automated systems supporting Air Traffic Services (ATS) units or aeronautical information systems, among others, to ensure the confidentiality, integrity and availability of the information as well as resilience of operations.
- Perform a risk analysis to evaluate cybersecurity threats and vulnerabilities, related to impacts on air traffic services.
- Review and update the technical and operational specifications of their systems considering that new technologies implemented in air traffic services provide greater efficiency and simplify operations management, however, they may be vulnerable to cyber threats. This review would help to mitigate cyber risks and ensure resilience.
- Monitor and analyse the exchange of information and the connections to identify possible cyber-attacks and establish the adequate protection measures for air traffic systems.
- Collaborate and cooperate with industry in order to adapt technical requirements to the development pace of new technologies and to ensure that hardware and software supporting air traffic systems are updated and prepared against cyber threats. Also, all interested parties (i.e. States, ANSPs and industry) need to collaborate in the design of the Standard Operating Procedures (SOPs) to ensure an adequate protection of their operations.
- Provide training and qualification for the personnel that manage ANS technical and operational areas for a correct provision of services. Staff should be knowledgeable and have the skills to carry out recovery plans in the event of a cyber incident.

2. Applicable Documents

- ICAO Annexes
- ICAO Document 8973 – Aviation Security Manual
- ICAO Document 9985 – ATM Security Manual
- ICAO Aviation Cyber Security Strategy
- ED 205 Process standard for Air Traffic Management / Air Navigation Services (ATM/ANS) ground systems security aspects of certification / declaration

3. Scope

This document covers the whole aviation functional structure and all aviation stakeholders such as Civil Aviation Authorities, Air Navigation Service Providers, Airports Operators and any other aviation organization that is part of the State Aviation System to ensure the implementation of cybersecurity procedures and practices in all services under the State oversight such as:

- Air Traffic Services Units (TWR, APP and ACC)
- Communication, Navigation and Surveillance data and infrastructure
- Digital information Systems (aeronautical information, meteorological information and other supporting decision-making information).
- Systems for aviation interoperability
- Others according with State services and operations.

This document applies to the whole aviation system locations and premises hosting:

- Information required by ATM services.
- Information technology (IT) infrastructure that ATM services rely on.
- Operational technology (OT) and Interconnected Industrial and Automated Controlled Systems (IACS).
- Extended services and partnership, and related Information System interconnections.
- All aviation personnel and external organizations having access to air navigation information, services and facilities.

4. Objectives

The overall objectives of this aviation system security Policy are:

- To ensure the resilience of the State Aviation System.
- To ensure information integrity, availability and confidentiality.
- To protect hardware/software supporting the aviation system infrastructure to reduce risks to all aviation State's services.
- To support the implementation of cybersecurity procedures and processes to all aviation infrastructure and services.
- To support civil aviation security, national security and defence and law enforcement.

5. Security Architecture Objective

In addition to the implementation of the best practices identified in the referenced documents, this document strongly recommends the identification, definition and implementation of security measures based on their criticality regarding safety and operability[1].

1 In information security the criticality is estimated with respect to CIA (confidentiality, integrity, availability) which could impact safety and operability.

6. ATM Security Documentation

Requirement ATMSP-001-01:

Based on this security policy, an information security management system shall be defined, implemented and maintained based on a risk management approach.

NB: ISO27001 and ISO27002 Standards provide approved process and best practices for ISMS

7. Risk Management

Requirement ATMSP-002-01:

ATM security shall be intelligence led, threat based and risk managed.

Requirement ATMSP-003-01:

Information security risk management shall be considered as an integral part of the overall system life cycle process.

Requirement ATMSP-004-01:

All ATM assets (data, systems, personnel...) shall have defined ownership.

Requirement ATMSP-005-01:

Defence in depth principles as defined in 5 – Security architecture objective, shall be part of the information security management.

Requirement ATMSP-006-01:

ATM Security Risk based approach shall implement technical security measures and operational security measures (policies and processes) to reduce risk to an acceptable level regarding:

- (Intentional) Successful cyber-attack,
- Human error,
- Accident or incident,
- Impact from natural disaster.

Requirement ATMSP-007-01:

The organisation in charge of physical or information ATM security shall ensure efficient and coordinated treatment of security risk.

Requirement ATMSP-008-01:

ATM information security risks shall be reviewed and monitored on a regular basis.

8. Security Governance and Organisation

Requirement ATMSP-009-01:

CAA shall designate the Appropriate Authority (AA) responsible for the overall ATM security.

Requirement ATMSP-010-01:

CAA designated ATM security responsible shall define at a minimum:

- Roles and responsibilities for ATM security risk management;
- Processes for risk management;
- Processes for incident and crisis management.

Requirement ATMSP-011-01:

Skills and competencies of personnel appointed to ATM security roles and responsibilities shall be kept up to date.

9. Human Resources

Requirement ATMSP-012-01:

Personnel shall be part of ATM security during all employment phases:

- Before employment: through measures such as background checks in accordance with local regulations;
- During employment: by developing a security culture through regular training and raising awareness; and
- After employment: by ensuring the respect of the de-provisioning process and reminding staff of non-disclosure commitments.

Requirement ATMSP-013-01:

Security personnel shall ensure that individuals with access to ATM facilities, controlled areas and ATM sensitive data do not constitute an unacceptable risk (as per Chapter 7 Risk Management).

10. Asset Management

Requirement ATMSP-014-01:

An inventory of ATM assets shall be developed and kept up to date.

Requirement ATMSP-015-01:

ATM shall classify its assets according to their criticality in order to implement appropriate means of protection.

Requirement ATMSP-016-01:

ATM data shall be by default classified with adequate level of classification.

Additional information: please refer to applicable national regulation

Requirement ATMSP-017-01:

ATM data shall be protected during storage, processing and exchange, in line with its sensitivity profile.

11. Access Control

Requirement ATMSP-018-01:

Access to any ATM assets shall be granted on:

- The verification of absence of unacceptable risk (as per Chapter 7 Risk Management); and
- A need-to-know basis.

12. Physical and Environmental Security of CNS/ATM Components

Requirement ATMSP-019-01:

ATM physical security shall safeguard IT, OT, IACS and CNS/ATM infrastructure, against unlawful interference and unauthorized access.

Requirement ATMSP-020-01:

ATM physical security shall identify zones hosting CNS/ATM assets according to their criticality regarding safety and operability.

Requirement ATMSP-021-01:

ATM physical security measures shall protect the CNS/ATM from unlawful or intentional interruption of services and operations.

Requirement ATMSP-022-01:

ATM physical security shall protect incoming and outgoing flows from storage zones and data centres.

13. Operations Security

Requirement ATMSP-023-01:

ATM cybersecurity organization shall ensure the coordination of security operations, monitoring and continuous improvement of information processing.

Requirement ATMSP-024-01:

ATM cybersecurity operations shall include IT, OT, IACS and CNS/ATMs infrastructure in the scope of security operations.

Requirement ATMSP-025-01:

ATM cybersecurity operations shall maintain the effectiveness of security measures throughout their lifecycle.

Requirement ATMSP-026-01:

ATM cybersecurity shall be operated from dedicated zones having dedicated physical and logical security perimeter.

Additional information: zones are to be defined in accordance with "zones and conducts" principles defined in IEC 62443.

Requirement ATMSP-027-01:

ATM cybersecurity shall prevent the exploitation of technical vulnerabilities on IT, OT, IACS and CNS/ATM infrastructure.

Requirement ATMSP-028-01:

ATM cybersecurity shall forbid the use of personal mobile devices for CNS/ATM activities.

Requirement ATMSP-029-01:

ATM cybersecurity shall ensure that professional mobile devices do not constitute an unacceptable risk to security (as per Chapter 7 Risk Management).

14. Communications Security

Requirement ATMSP-030-01:

ATM cybersecurity shall maintain an up to date mapping of networks and their interconnections.

Requirement ATMSP-031-01:

ATM networks shall be logically or physically segregated based on their criticality regarding safety and operability.

Requirement ATMSP-032-01:

ATM cybersecurity shall ensure that wireless technologies and access to the Internet do not constitute an unacceptable risk to safety and security (as per Chapter 7 Risk Management).

15. System Acquisition, Development and Maintenance

Requirement ATMSP-033-01:

ATM cybersecurity shall ensure that information security is an integral part of CNS/ATM information systems throughout the entire lifecycle.

Additional information: This also includes the requirements for information systems which provide ATM services over public networks.

Requirement ATMSP-034-01:

ATM cybersecurity shall ensure that CNS/ATM information systems are designed based on the following principles (list not exhaustive):

- No single, nor common point of vulnerability;
- Definition and implementation of security coding rules;
- Vulnerability management on COTS software and hardware;
- Implementation of industry standards and recommendations (NIST, OWASP, …).

16. Suppliers and Partners Relationships

Requirement ATMSP-035-01:

ATM cybersecurity shall provide End-to-End security from supply chain to partners in the scope of CNS/ATM cybersecurity management system.

Requirement ATMSP-036-01:

ATM cybersecurity shall ensure relationships with external entities do not constitute an unacceptable risk (as per Chapter 7 Risk Management).

17. Security Incident Management

Requirement ATMSP-037-01:

ATM cybersecurity shall ensure a consistent and effective approach to the management of CNS/ATM security incidents, including communication on security events and weaknesses.

Requirement ATMSP-038-01:

Safety and Business Continuity shall be the main priorities of ATM security incident management.

18. Security Aspects of Business Continuity Management

Requirement ATMSP-039-01:

ATM Business continuity shall be designed in accordance with Risk Management outcomes.

Requirement ATMSP-040-01:

ATM cybersecurity shall establish a consistent, effective and common strategy to manage CNS/ATM security and safety through integration of all Stakeholders with common efforts, sharing information, to complete their operational objectives.

19. Protection of Personal Data

Requirement ATMSP-041-01:

ATM cybersecurity shall ensure the privacy and protection of personally identifiable information in accordance with applicable regulations.

20. Compliance

Requirement ATMSP-042-01:

CNS/ATM information systems shall receive recognized security validation qualification before entry into service in compliance with ED 205 Process standard for Air Traffic Management / Air Navigation Services (ATM/ANS) ground systems security aspects of certification / declaration.

Additional information: recognised accreditation process is to be defined at national level and made applicable for critical infrastructures.

Requirement ATMSP-043-01:

CNS/ATM information systems security validation shall be controlled on a regular basis.

Requirement ATMSP-044-01:

ATM cybersecurity shall ensure that any deviation, detected through the validation process, does not constitute an unacceptable risk (as per Chapter 7 Risk Management).

Referenced Documents

Reference	Title	Issue	Date
ISO27001-2013	Information Security Management	2013	
ISO27002-2013	Information technology – Security techniques	2013	
NIST SP 800-53	Security and Privacy Controls for Federal Information Systems and Organisations	R4	2015
IEC-62443	Industrial Network and Systems Security		
Doc 9985	Air Traffic Management Security Manual	1	2013
	Aviation Cybersecurity Strategy – ICAO		Oct 2019
ED-205	Process standard for Air Traffic Management / Air Navigation Services (ATM/ANS) ground systems security aspects of certification / declaration		Mar 2019
	Reference: Manual for National ATM Security Oversight (EUROCONTROL)	2.0	Oct 2013
	Strategy for Cybersecurity in Aviation (European Strategic)	1.0	Sep 2019
CANSO	CANSO Cyber Security and Risk		Jun 2014
CANSO	Assessment Guide		Sep 2020
	CANSO Cyber Risk Assessment Guide		

Terms and Definition

Reference	Title
ASSET	An asset is anything the organization puts value in. The term asset encompasses, but is not limited to personnel, digital values, information technology resources, technological legacy, facilities, interconnected industrial and automated controlled systems or operational technology, products, programs, information security assessments and branding. Assets can be categorized as follows: • Tangible Asset: software, hardware, equipment, facilities, people • Non tangible asset: business processes and information
ATM	Air Traffic Management
ATM Security	ATM Cybersecurity organization, management and activities involved in the protection of ATM functional infrastructure against Intentional Unauthorized Electronic Interference
CNS/ATM	Communications, navigation, and surveillance systems, employing digital technologies, including satellite systems together with various levels of automation, applied in support of a seamless global air traffic management system
IACS	Interconnected Industrial and Automated Controlled Systems [based on: ISA/IEC 62443]
IT	Information Technology
IUEI	A circumstance or event with the potential to affect an aircraft due to human action resulting from unauthorized access, use, disclosure, denial, disruption, modification, or destruction of information and/or aircraft system interfaces. This includes the consequences of malware and forged data and the effects of external systems on aircraft systems, but does not include physical attacks or electromagnetic disturbance. [based on: ED-202A / DO-326A]
Operability	Operability is the ability to keep a piece of equipment, a system or a whole industrial installation in a safe and reliable functioning condition, according to pre-defined operational requirements.
OT	Operational Technology
Risk	Combination of the probability of an event and its consequence. [based on: ISO27000-2018 and NIST SP 800-53-r4] A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: • the adverse impacts that would arise if the circumstance or event occurs; and • the likelihood of occurrence. Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. Adverse impacts to the Nation include, for example, compromises to information systems that support critical infrastructure applications or are paramount to government continuity of operations as defined by the Department of Homeland Security. [Based on NIST SP 800-12 Rev. 1]
Safety	ICAO Doc 9859: Safety is the state in which the possibility of harm to persons or property damage is reduced to, and maintained at or below, an acceptable level through a continuing process of hazard identification and risk management.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. [CNSS Inst. 4009, Adapted] [Source: NIST SP800-53, Rev 2] A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. [Source: ED-202 / DO-326]

CANSO

canso.org