International Civil Aviation Organization
North American, Central American and Caribbean Office

WORKING PAPER

NACC/WG/7 — WP/34
30/08/22

Seventh North American, Central American and Caribbean Working Group Meeting (NACC/WG/7)
ICAO NACC Regional Office, Mexico City, 30 August - 1 September 2022

Agenda Item 4: **NACC/WG Work Programme Update to 2024**
4.5 Emerging technologies and regional challenges

CYBERSECURITY IN AIR NAVIGATION SERVICES

(Presented by the Secretariat)

EXECUTIVE SUMMARY	
This working paper provides a summary on the available information on cybersecurity in air navigation services.	
Action:	Suggested actions are presented in Section 3.
Strategic Objectives:	• Safety
References:	• ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation, December 2020 https://www.icao.int/NACC/Pages/meetings-2020-aci.aspx • Second ICAO/CANSO/AIRBUS Webinar on Aviation Cybersecurity Implementation-Cybersecurity Policy Manual https://www.icao.int/NACC/Pages/meetings-2021-canso02.aspx • Sixth North American, Central American and Caribbean Working Group Meeting (NACC/WG/6), online, 25 – 27 August 2021 https://www.icao.int/NACC/Pages/meetings-2021-naccwg6.aspx.

1. Introduction

1.1 Air navigation services have evolved in the last decade, implementing highly digital and automated technologies that require the implementation of other security mechanisms than those we have known to date.

1.2 Cyber technology and systems have become essential to modern society, being a component of many activities that have become dependent on information technology. Along with the benefit of cyber technologies, insecurities arise that affect all systems and infrastructures.

1.3 The cyber-threat and cyber-attack have a transnational component and effect, since global systems are interconnected. In addition, the complexity of the action has implications for various actors at the national, regional and international levels.

1.4 It is in this environment of cyber-insecurity that civil aviation carries out its activity. Civil aviation relies heavily on cyber technology that is used to increase the safety and efficiency of air transport. However, the interconnectivity of systems and the dependence on technology have created the optimal premises for new risks to emerge.

1.5 The aviation sector uses a wide range of interconnected computer-based systems, ranging from air navigation systems, aircraft on-board communication and control systems, airport ground systems, flight information, security checks and many others that are used on a daily basis and for all aviation-related operations. The trend in the aviation sector is to become increasingly digital. Digitization brings new dangers, as interactions between people and systems make risk more difficult to predict.

1.6 Recognizing the urgency and importance of protecting critical civil aviation infrastructure, information and communication technology systems and data against cyber threats, ICAO is committed to developing a robust cybersecurity framework. The 40 Session of the ICAO Assembly adopted *Resolution A40-10 - Addressing cybersecurity in civil aviation*. The resolution addresses cybersecurity through a horizontal, transversal and functional approach, reaffirming the importance and urgency of protecting critical infrastructure systems and civil aviation data against cyber-threats, and calls on States to apply the ICAO Cybersecurity Strategy.

1.7 Aviation cybersecurity strategy encompasses rests on seven pillars:

1. International cooperation
2. Governance
3. Effective legislation and regulations
4. Cybersecurity policy
5. Information sharing
6. Incident management and emergency planning
7. Capacity building, training and cybersecurity culture

1.8 The full document is available at the following link:

https://www.icao.int/cybersecurity/Documents/AVIATION%20CYBERSECURITY%20STRATEGY.EN.pdf#search=Aviation%20cybersecurity%20strategy

1.9 Since 2020, the ICAO NACC Regional Office has made an alliance with CANSO and AIRBUS and focused on the development of guidance documentation that allows States to evaluate air navigation systems and, based on this, develop their own cybersecurity policy customized to their operations. The document is a manual called: Air Traffic Management Cybersecurity Policy Template.

1.10 The manual is prepared following the recommendations of resolution *A40-10 - Addressing cybersecurity in civil aviation*, and under the ICAO Cybersecurity strategy, based on pillar number 4 "Cybersecurity Policy".

1.11 The NACC/WG is requested to adopt the document so that it can be used by the CAR region.

2. Cybersecurity Policy Template for Air Traffic Management

2.1 The objectives of this document are:

1. Contribute to the resilience of the State aviation system.
2. Provide support for the integrity, availability, and confidentiality of information.
3. Protect the hardware/software that supports the aviation system infrastructure to reduce risks for all State services.
4. Support the implementation of cybersecurity procedures and processes for all infrastructure and services.
5. Support cybersecurity and resilience of civil aviation.

2.2 The document lists a series of requirements that States must assess regarding their architecture and operations. Identifies the infrastructure and systems that are the core of its operations and implements mechanisms that ensure its protection and, most importantly, the continuity of its operations.

2.3 The document is in the **Appendix** to this working paper. This second version incorporates comments from the ICAO Air Navigation and Air Transport Offices.

2.4 A checklist has also been integrated into this new version that serves as a guide for the State to evaluate the requirements that it meets or does not meet according to its operations.

2.5 The ICAO NACC Regional Office has held a series of events aimed at understanding what cybersecurity means, and identifying threats to aviation operations, but it is necessary for States to take very seriously the activities that must be carried out in regarding this area.

2.6 Cybersecurity requires a commitment from States to allocate resources in all areas, from human to financial. However, prior to the development of projects aimed at this area, it is necessary for States to carry out an analysis of their operations and the Air Traffic Management Cybersecurity Policy Template supports this activity.

2.7 Projects in this area require an investment that must be supported by data that supports decision-making and the evaluation of their operations. The staff will support the State in defining the activities that it needs to develop.

2.8 The ICAO NACC Regional Office thanks CANSO and AIRBUS for this joint work. It is important to emphasize that the joint work between the organizations allows them to take advantage of the experts, experience and work more effectively on tasks of common interest and for the benefit of the States.

3. Suggested Actions

3.1 The meeting is invited to:

a) approve the adoption of the document as a Regional Guide for States;

b) designate Point of Contact (PoC) personnel by States to work directly with them;

c) work with the ICAO Regional Office in the scheduled activities to deal with cybersecurity issues addressed to air navigation services; and

d) other applicable action.

— — — — — — — — — — —

In cooperation with

ICAO canso AIRBUS

Air Traffic Management Cybersecurity Policy Template

DISCLAIMER

The information contained in this publication is subject to on-going review in the light of changing ICAO Standards and regulations and other important information provided by ICAO, CANSO and Airbus.

This publication has to objective to help CAR and Latin American States in the evaluation and start their work about cybersecurity.

Latin America and CAR Region has been implemented State of the art technology to support the evolution of their air navigation operations, in that sense is really important to support this evolution incorporating information to support States in the security cybersecurity implementation.

Cyber-attack does not stop, every year the percentage of incidents increase, include aviation sector.

This publication does not replace any other national or regional regulation.

This publication expressly disclaim any and all liability to any person or entity, whether a user of this publication or not, in respect of anything done or omitted, and the consequences of anything done or omitted, by any such person or entity in reliance on the contents of this publication.

The mention of specific companies and products in this publication does not imply that they are endorsed or recommended by any of the above in preference to others of a similar nature, which are not mentioned.

No part of this publication may be reproduced, recast, reformatted or transmitted in any form by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system, without the prior written permission of the authors.

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:

- **Javier Vanegas,** Director, Latin America and Caribbean Affairs, CANSO
- **Shayne Campbell**, Safety Programme Manager, CANSO
- **Eduardo Garcia**, Manager European ATM Coordination and Safety, CANSO
- **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

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 affect the safety and security of flights and the reputation of civil aviation in the public eye. As such, ICAO addressed this emerging threat to civil aviation through resolution A40-10: "Addressing Cybersecurity in Civil Aviation" during the A40 Assembly- 40th Session in Montreal, from September 24 to October 4, 2019.

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 systems (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 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, ICAO considers Cybersecurity as an interrelated matter 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.

Add here the comments

1. How to use this document

This document does not replace any Standards and Recommended Practices (SARPS) , no PANS- ICAO or National Regulation. This document support the previous listed documents.

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 support the confidentiality, integrity and availability of the information as well as resilience of operations.

- Perform and maintain 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 analyze 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 contribute the resilience of the State Aviation System.
- To provide support to 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 air navigation-infrastructure and services.
- To support civil aviation cyber security and resilience.

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 should be defined, implemented and
maintained based on a risk management approach.

NB: ISO27001 and ISO27002 Standards provide approved processes and best practices for ISMS and other available documents in the national regulations, and organizations within the States.

7. Risk Management

Requirement ATMSP-002-01:

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

Requirement ATMSP-003-01:

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

Requirement ATMSP-004-01:

All ATM assets (data, systems, personnel…) should have defined responsibility.

Requirement ATMSP-005-01:

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

Requirement ATMSP-006-01:

ATM Security Risk based approach should 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 organization in charge of physical or information ATM security should ensure efficient and coordinated treatment
of security risk. Improve this part

Requirement ATMSP-008-01:

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

8. Security Governance and Organization

Requirement ATMSP-009-01:

States should designate the Appropriate Authority (AA) responsible for the overall ATM security.

Note: This requirement will depend on the national regulations and agreements.

Requirement ATMSP-010-01:

Designated ATM security responsible should 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 should be kept up to date.

9. Human Resources

Requirement ATMSP-012-01:

Personnel should 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 Cybersecurity 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 should 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 should be developed and kept up to date.

Requirement ATMSP-015-01:

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

Requirement ATMSP-016-01:

ATM data should be identify critical data ~~classified~~ adequately.

Note: Additional information: please refer to applicable national

regulation

Requirement ATMSP-017-01:

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

11. Access Control

Requirement ATMSP-018-01:

Access to any ATM assets should 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 should safeguard IT, OT, IACS and CNS/ATM infrastructure, against unlawful interference and unauthorized access.

Requirement ATMSP-020-01:

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

Requirement ATMSP-021-01:

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

Requirement ATMSP-022-01:

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

13. Operations Security

Requirement ATMSP-023-01:

ANSP cybersecurity department organization should ensure the coordination of cyber security operations, monitoring and continuous improvement of information processing.

Requirement ATMSP-024-01:

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

Requirement ATMSP-025-01:

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

Requirement ATMSP-026-01:

ATM cybersecurity should 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:

ANSP CD ATM cybersecurity should protect against the exploitation of technical vulnerabilities on IT, OT, IACS and CNS/ATM infrastructure.

Requirement ATMSP-028-01:

ATM cybersecurity should forbid the use of personal mobile for regular CNS/ATM activities.

Requirement ATMSP-029-01:

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

Requirement ATMSP-031-01:

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

Requirement ATMSP-032-01:

ATM cybersecurity should 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 should ensure that information security is an integral part of CNS/ATM 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 should ensure that CNS/ATM systems are designed based on the following principles (list not exhaustive):

- No single, nor common point of failure;
- 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 should provide End-to-End security from supply chain to partners in the scope of CNS/ATM
cybersecurity management to cover all CNS/ATM systems.

Requirement ATMSP-036-01:

ATM cybersecurity should 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 should ensure a consistent and effective approach to the management of CNS/ATM

Cybersecurity incidents, including communication on security events and weaknesses.

Requirement ATMSP-038-01:

Safety and Business Continuity should be the main priorities of ATM Cybersecurity incident management.

18. Security Aspects of Business Continuity Management

Requirement ATMSP-039-01:

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

Requirement ATMSP-040-01:

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

20. Compliance

Requirement ATMSP-042-01:

CNS/ATM information systems should 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 the national level and made applicable for critical infrastructures)

Requirement ATMSP-043-01:

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

Requirement ATMSP-044-01:

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

20. Compliance

The **Attachment** to this document incorporates the checklist to be used for the evaluation of your aviation system regarding the implementation of Cybersecurity.

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	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	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
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]

In cooperation with

ICAO

Air Traffic Management Cybersecurity Policy Template Checklist

ATTACHMENT

Introduction

The present document is a checklist that it has the aim to review all requirements cybersecurity implementation about the Document Air Traffic Management Cybersecurity Police Template.

The Document is not a mandatory requirements implementation, but it contains important information that will help you to support the development of your own Cybersecurity Police Manual.

Scope

This document covers the whole aviation functional structure and all aviation stakeholders such as Civil Aviation Authorities, Air Navigation Service Providers and any entity or 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.

In cooperation with

ICAO

Air Traffic Management Cybersecurity Policy Template Checklist

State:
Point Of Contact (s): Please Introduce Name, e-mail and telephone number of each person designate by the State.

CYBERSECURITY CHECKLIST

1. ATM Security Documentation

-> ATM Cybersecurity Policy Template, Chapter 6

		Yes	In Progress %	No
1.1	Have you established an Information Security policy for your organization?			
1.2	Have you already set up ISMS for your organization?			
1.3	Is your ATM documentation: • Implemented? • And maintained? • Based on a risk management approach?			
	Have you identified and scoped your infrastructure (e.g. as “IT”, “OT”, and “IACS”) so its security can be appropriately and proportionately managed?			

IT Infrastructure	OT and IACS Infrastructure

Air Traffic Management Cybersecurity Policy Template Checklist

2. Risk Management

-> ATM CYBERSECURITY POLICY TEMPLATE, CHAPTER 7

		Yes	In progress %	No
2.1	Is security addressed in all phases of System life cycle?			
2.2	Do you have a defined and repeatable risk management procedure (methodology) in place?			
2.3	Are security risks: • Tracked? • Monitored? • And periodically reviewed?			
		Yes	**In progress %**	**No**
2.4	Have you taken steps to process vulnerability management on systems?			
2.5	Have you identified all ATM assets (data, systems, personnel...) and established control procedures for them?			
2.6	Have you empowered the right personnel for making treatment decisions on Security risks?			
2.7	Do you have Information Security Management processes defined? (addressing all security activities)			
2.8	Do you have established technical security measures and operational security measures (policies and processes)? The intention of this is to reduce risk to an acceptable level regarding to human error, Accident or incident, Impact from natural disaster and others.			
2.9	Do you have identified interfaces to ensure efficient and coordinated treatment of security risk about ATM security?			
2.10	Have you established Risk management process covering ATM information security risks, with regular review and monitoring?			

Air Traffic Management Cybersecurity Policy Template Checklist

3. Security Governance and Organization -> ATM Cybersecurity Policy Template, Chapter 8				
		Yes	**In progress %**	**No**
3.1	Have you established an appropriate authority for ATM security management at a Unit level?			
3.2	Have you established Roles and Responsibilities within ATM security risk management?			
3.3	Have you implemented defined processes for Threat Intelligence and monitoring			
3.4	Have you implemented defined processes for incident and crisis management?			
4. Human Resources (Security measures during all employment phases) -> ATM Cybersecurity Policy Template, Chapter 9				
		Yes	**In progress %**	**No**
4.1	Before employment: do you use measures such as background checks in accordance with local regulations?			
4.2	During employment: do you develop a security culture through regular training and raising awareness?			
4.3	After employment: do you protect yourself by ensuring the de-provisioning process for access, and by reminding staff of nondisclosure Commitments (where allowed by law)?			
4.4	Do you have procedures to assign and limit staff access according to their responsibilities?			
5. Asset Management -> ATM Cybersecurity Policy Template, Chapter 10				
		Yes	**In progress %**	**No**
5.1	Have you taken an inventory of ATM assets and kept it up to date?			
5.2	Does the inventory include criticality evaluation (regarding safety and operability) for each asset?			
5.3	Have you considered logical and physical access, and made sure there is consistency between them?			

Air Traffic Management Cybersecurity Policy Template Checklist

		Yes	In progress %	No
5.4	Is all ATM data considered and classified, and protected to an adequate level?			
5.5	Do you have procedures to ensure that all ATM data will be protected during storage, processing and exchange, in line with its sensitivity profile?			

6. Access Control

-> ATM Cybersecurity Policy Template, Chapter 11

		Yes	In progress %	No
6.1	Is all access to ATM assets through a suitable access verification process, to avoid unacceptable risk?			
6.2	Do you have controls covering physical and logical access to systems?			

7. Physical and Environmental Security of CNS/ATM Components

-> ATM Cybersecurity Policy Template, Chapter 12

		Yes	In progress %	No
7.1	Have you ensured that ATM physical security safeguards IT, OT, IACS and CNS/ATM infrastructure against unlawful interference and Unauthorized access?			
7.2	Have you ensured that ATM physical security identifies zones hosting CNS/ATM assets according to their criticality (from safety and operability perspectives)?			
7.3	Have you implemented ATM physical security measures to protect all CNS/ATM from unlawful or intentional interruption of services and operations?			
7.4	Have you implemented ATM physical security to protect incoming and outgoing information flows between storage zones and data centres?			

Air Traffic Management Cybersecurity Policy Template Checklist

8. Operations Security -> ATM Cybersecurity Policy Template, Chapter 13				
		Yes	**In progress %**	**No**
8.1	Have you established trust zones?			
8.2	Have you established procedures to ensure ATM cybersecurity coordination of security operations, monitoring and continuous improvement of information processing?			
8.3	Have you ensured that ATM cybersecurity operations include IT, OT, IACS and CNS/ATMs infrastructure in the scope of security operations?			
8.4	Have you implemented ATM cybersecurity operations to maintain the effectiveness of security measures throughout their lifecycle?			
8.5	Have you established a security perimeter through ATM cybersecurity zones for physical and logical zones?			
		Yes	**In progress %**	**No**
8.6	Do you have procedures to prevent the exploitation of technical vulnerabilities on IT, OT, IACS and CNS/ATM infrastructure?			
8.7	Do you have security controls around the use of personal mobile devices for CNS/ATM activities (e.g. is their use forbidden)?			
8.8	Do you take steps to ensure that personal mobile devices do not represent a risk for the security of CNS/ATM activities (e.g. plugging in a personal device to operational equipment to charge)?			

Air Traffic Management Cybersecurity Policy Template Checklist

9. Communications Security -> ATM CYBERSECURITY POLICY TEMPLATE, CHAPTER 14				
		Yes	**In progress %**	**No**
9.1	Do you collect and maintain an up-to-date mapping of networks and their interconnections?			
9.2	Do you ensure ATM networks are logically or physically segregated based on their criticality regarding safety and operability?			
9.3	Do you take steps to ensure that wireless technologies and access to the Internet do not constitute an unacceptable risk to safety and security?			
10. System Acquisition, Development and Maintenance -> ATM CYBERSECURITY POLICY TEMPLATE, CHAPTER 15				
		Yes	**In progress %**	**No**
10.1	Is information security is an integral part of your management of CNS/ATM information systems throughout the entire lifecycle?			
10.2	Do you ensure that your CNS/ATM information systems are designed based on the following principles: • No single, nor common point of vulnerability? • Defined and verified use of security coding rules? • Vulnerability management on COTS software and hardware? • The use of appropriate industry standards and recommendations (e.g. NIST, OWASP, EUROCAE/RTCA, etc.)?			

Air Traffic Management Cybersecurity Policy Template Checklist

11. Suppliers and Partners Relationships

-> ATM Cybersecurity Policy Template, Chapter 16

		Yes	In progress %	No
11.1	Do you evaluate the security maturity of suppliers and partners prior to contract?			
11.2	Does your risk management process also address risk on suppliers?			

12. Security Incident Management

-> ATM Cybersecurity Policy Template, Chapter 17

		Yes	In progress %	No
12.1	Do you have communication procedure and communication lists in case of security incident or weakness identification?			

13. Security Aspects of Business Continuity Management

-> ATM Cybersecurity Policy Template, Chapter 18

		Yes	In progress %	No
13.1	Do you have defined interfaces between ATM Business continuity and Risk Management processes?			
13.2	Do you perform crisis management exercise and test based on ATM security case?.			

14. Protection of Personal Data

-> ATM Cybersecurity Policy Template, Chapter 19

		Yes	In progress %	No
14.1	Do you have defined interface between DPO and ATM security process.			

15. Compliance

-> ATM Cybersecurity Policy Template, Chapter 20

		Yes	In progress %	No
15.1	Do you perform regular Third party Security audit of ATM/CNS information systems.			

— END —