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

WORKING PAPER

AIM/TF/7 — WP/02
23/07/24

Seventh North American, Central American and Caribbean Working Group (NACC/WG) Aeronautical Information Management Implementation Task Force Meeting
(AIM/TF/7)
(Willemstad, Curaçao, 30 July – 2 August 2024)

Agenda Item 2: **AIM Data & Cybersecurity**

CYBERSECURITY CONCEPTS AND APPLICATION IN AIM

(Presented by the Secretariat)

Executive Summary	
The purpose of this Working Paper is to present the ICAO concept and role of cybersecurity in the aviation sector, to identify deficiencies in its provision and regulation Data and information applicable to AIM, and to formulate proposals aimed at improving standards and to ensure the proper level of aviation cybersecurity.	
Action:	Suggested action is presented in Section 5.
Keywords	Cybersecurity, cybercrime, aviation cybersecurity, safety of flights, critical information and data infrastructure.
Strategic Objectives:	• Strategic Objective 1 – Safety • Strategic Objective 2 – Air Navigation Capacity and Efficiency
References	• Resolution A41-19 on Addressing Cybersecurity in Civil Aviation • ICAO "Aviation Cybersecurity Strategy" • ICAO "Cybersecurity Policy Guidance" • Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) • Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol)

1. Introduction

1.1 Cybersecurity in the aviation sector has acquired relevance in the growing level of development of information technologies in the aviation sector, and in particular in AIM for the management and exchange of Data, so an analysis is necessary detail of the existing international standards and norms to guarantee the aviation cybersecurity and their implementation with various initiatives and technologies in this matter, starting with the study of the Documents with the strategies and plans of the ICAO, to face the problems of the cybercrimes in this area of aviation that represent significant risks to security.

1.2 The Concept of Cybersecurity and its implications for the Aviation Sector and digitalization in the air transport industry has enabled the relevant entities to provide better services to their customers. At the same time, the level of exposure to threats, especially cyberattacks, also increased. Based on the above, it should be noted that key concepts and categories are considered in the process of analysis and presentation of the material. To begin with, it is important to determine how the term information security is understood, since this concept can be understood from several points of view.

2. Discussion

2.1 The object of the study is relations arising concerning aviation security and cybersecurity in the aviation sector.

2.2 As for the domestic States legislation, information security is a high priority of protection of the vital interests of both a person and society and the State by itself. In such a situation, the harm by providing incomplete, inaccurate, and untimely data and information is prevented in every possible way. In addition to providing the specified "negative" information to the corresponding malicious actions, this regulatory act also includes the negative information impact and the corresponding consequences of the use of information technology, unauthorized distribution, use and violation of confidentiality, accessibility, the integrity of information

2.3 Thus, it should be noted that not all information security issues are related to the notion of "cybersecurity." After all, there are aviation systems, isolated from networks, and included in the technological circuit of air traffic control.

2.4 That is why ensuring data security in them must be successfully harmonized with the data/information security fundamentals of a higher-level system. The constantly mentioned cyberspace can be defined as a global area in the data/information environment, which included information systems, interdependent networks of information infrastructure systems, telecommunications networks, and computer systems, and the like.

3. Solutions for cybersecurity issues in the aviation sector

3.1 The problem of aviation cybersecurity forced the aviation authorities of many States, as well as international organizations like ICAO, to make every effort to create the appropriate conditions for ensuring security in this risk Area.

3.2 During the **41 ICAO's Assembly**, held at Headquarters (Montreal), the **Resolution A41-19** on **Addressing Cybersecurity in Civil Aviation** was adopted (**Appendix A**), which declared the need to jointly address this problem under the Beijing Convention, to urge all States to implement the ICAO “Aviation Cybersecurity Strategy”, October 2019 (**Appendix B**). The main aim of the Resolution is to organize cooperation between not only among States but international Organizations and Industry to develop policies (see ICAO “Cybersecurity Policy Guidance”, January 2022 – **Appendix C**) to ensure a holistic approach to aviation cybersecurity.

3.3 In addition and considering that the Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) would enhance the global legal framework for dealing with cyber-attacks on international civil aviation as crimes and therefore wide ratification by States of those instruments would ensure that such attacks would be deterred and punished wherever in the world they occur.

3.4 Furthermore, in ICAO TRAINAIR PLUS Program it was proposed a course of “Fundamentals of Cybersecurity for Aviation". The course aims to train aviation professionals in identifying existing and potential cyber threats so that these participants can more effectively and quickly respond to such problems. Thus, the specified training will help ensure the safety of air travel for passengers around the world. The first recipients of new knowledge will be representatives of civil aviation regulatory bodies, civil airlines, and airports,

3.5 To achieve this, a group of principles and methods of a special mechanism will be applied, which includes seven key components, namely:

a)	cooperation between States and organizations
b)	the exchange of important data between these entities
c)	the development of effective legislation
d)	the introduction of a transparent cyber policy
e)	joint planning of reactionary actions in case of incidents and emergencies
f)	the formation of a culture of cybersecurity
g)	in parallel with the training of professionals in this area

4. Conclusions

4.1 Now a days cybersecurity is one of the key issues in the aviation industry. Airlines and other international organizations operating in this area are actively interacting and implementing various methods and technologies to ensure a sufficient level of safety and security, both physical and virtual (digital). For most States in the world, the air transport sector is a part of the critical infrastructure of the States. Therefore, many civil aviation authorities are also concerned about the implementation of new standards and regulations to address risks in cyberspace.

4.2 But at the same time, industry and organizations (ICAO, IFAIMA, ACI, IATA, CANSO and others) develop relevant initiatives to face cyber-threats in the field of air navigation and transport that are real and generally recognized, both individual organizations and all States are actively cooperating with the aim of mutual education, information and protection in the area under consideration.

4.3 The world aviation community is faced with the need to develop a system of coordinated measures and a special decision-making procedure for ensuring the protection of the global aviation industry system from cyber-attacks. It is important not only to implement such actions but also to learn how to successfully combine them with periodic acts to protect the components of aviation cyberspace from external influences.

4.4 Finally, in the Secretariat´s opinion, is the application of ICAO recommended practices, as well as harmonization of the national regulatory framework with international principles and standards in the field of cybersecurity. The resolution of cybersecurity issues in the civil aviation sector requires a concerted effort by all players in the aerospace industry (see **Appendix D**). We can safely say that high-quality, the aviation sector is increasingly reliant on the availability, integrity and confidentiality of information, data, and systems protection against cyberattacks in aviation should become a strategic priority for both the world aviation community and the national safety and security for each individual State.

5. Suggested actions

5.1 The Meeting is invited to:

a) take note of the information presented in this Working Paper and in its **Appendixes A**, **B, C and D**

b) provide comments on the current status of Cybersecurity actions according **ICAO Resolution A41-19** on **Addressing Cybersecurity in Civil Aviation** as requested in **Appendix A**; and

c) suggest additional actions if appropriate.

— — — — — — — — — — —

Resolution A41-19: Addressing Cybersecurity in Civil Aviation

Whereas the global aviation system is a highly complex and integrated system that comprises systems that are critical for the safety and security of civil aviation operations;

Noting that the aviation sector is increasingly reliant on the availability, integrity and confidentiality of information, data, and systems;

Mindful that cyber threats to civil aviation are rapidly and continuously evolving, that aviation continues to be a target for perpetrators in the cyber domain as in the physical one, and that cyber threats can evolve to affect critical civil aviation systems worldwide;

Recognizing that not all cybersecurity events affecting the safety of civil aviation are unlawful and/or intentional;

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity challenges and solutions and noting that cyber risks can simultaneously affect a wide range of aviation areas and spread rapidly;

Reaffirming the obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation;

Considering that the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft (Beijing Protocol) would enhance the global legal framework for dealing with cyber-attacks on international civil aviation as crimes and therefore wide ratification by States of those instruments would ensure that such attacks would be deterred and punished wherever in the world they occur;

Reaffirming the importance and urgency of addressing the cybersecurity and cyber resilience of civil aviation's critical systems, data, and information against cyber threats and hazards, including common interfaces between civil and military aviation;

Considering the need to work collaboratively towards the development of an effective and coordinated global framework to address aviation cybersecurity and to support the cybersecurity and cyber resilience of the global aviation system to cyber threats that may jeopardize the safety and/or security of civil aviation;

Recognizing ICAO's leadership and work in the fields of aviation cybersecurity and cyber resilience across the different aviation disciplines;

Recognizing that aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to ensure the consistency and full interoperability of protection measures and risk management systems;

Recognizing the importance of developing clear national governance and accountability for civil aviation cybersecurity, including the designation of a competent national authority responsible for aviation cybersecurity in coordination with concerned national authorities and agencies; and

Acknowledging the value of relevant initiatives, action plans, publications and other media designed to address cybersecurity issues in a collaborative and holistic manner.

The Assembly:

1. *Urges* Member States to adopt and ratify the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol) as a means for dealing with cyberattacks against civil aviation;

2. *Calls upon* States and industry stakeholders to take the following actions to address cyber threats to civil aviation:

a) implement the ICAO Aviation Cybersecurity Strategy, and make use of the ICAO Cybersecurity Action Plan as a tool to support the implementation of the Aviation Cybersecurity Strategy;

b) designate the authority competent for aviation cybersecurity, and define the interaction between that authority and concerned national agencies;

c) define the responsibilities of national agencies and industry stakeholders with regard to cybersecurity in civil aviation;

d) develop and implement a robust cybersecurity risk management framework that draws on relevant safety and security risk management practices, and adopt a risk-based approach to protecting critical civil aviation systems, information, and data from cyber threats;

e) establish policies and instruments, and allocate resources to ensure that, for critical aviation systems: system architectures are secure by design; systems are protected and resilient; data is secured and available in storage and while in transfer; system monitoring, and incident detection and reporting, methods are implemented; incident recovery plans are developed and practiced; and forensic analysis of cyber incidents is carried out;

f) encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;

g) encourage civil/military cooperation with regard to identifying, protecting, and monitoring common vulnerabilities and data flows at interfaces between civil and military aviation systems, and collaborate in response to common cyber threats and recovery from cyber incidents;

h) develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;

i) design and implement a robust cybersecurity culture across the civil aviation sector;

j) encourage States to continue contributing to ICAO in the development of international Standards, strategies, and best practices to support advancing aviation cybersecurity and cyber resilience; and

k) continue collaborating in the development of ICAO's cybersecurity framework according to a horizontal, cross-cutting and functional approach involving aviation safety, aviation security,

facilitation, air navigation, communication, surveillance, air traffic management, aircraft operations, airworthiness, and other relevant disciplines.

3. *Instructs* ICAO to:

a) continue to promote the universal adoption and ratification of the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol); and

b) continue to ensure that cybersecurity and cyber resilience matters are considered and coordinated in a cross-cutting manner through the new mechanism in ICAO to address aviation cybersecurity.

APPENDIX B

Cybersecurity Policy Guidance

Published by authority of the Secretary General

January 2022

International Civil Aviation Organization

1. Introduction

This guidance is in line with the ICAO Aviation Cybersecurity Strategy[1], and the Cybersecurity Action Plan[2], which action item CyAP0.1 recommends that the International Civil Aviation Organization (ICAO) develops a model Cybersecurity Policy for reference by Member States and industry when developing their own national/internal policies.

The model Cybersecurity Policy is included in Appendix A to this guidance.

2. Scope

The model Cybersecurity Policy outlined in Appendix A of this document addresses the protection and resilience of international civil aviation's critical infrastructure against cyber threats, and the multilateral collaboration requirement within civil aviation as well as with external authorities such as military, cybersecurity, and national security.

3. Objectives

The model Cybersecurity Policy is intended to serve as a guide to help States and industry focus resources and actions to achieve a systemic approach to cybersecurity in civil aviation, including current and legacy systems. The ultimate goal is for States and stakeholders to be able to develop a system-of-systems approach that enables civil aviation to be protected against cyber threats, and to respond to and recover from cyber incidents in a timely fashion, and, therefore, to withstand new threats without significant disruptions.

The main outcomes expected from implementing a Cybersecurity Policy are:

3.1 Ensure civil aviation is protected against cyber threats

The protection of civil aviation against cyber-attacks is addressed through the implementation of ICAO cybersecurity Standards and Recommended Practices, procedures, and guidance material. It includes the implementation of robust risk management practices, the identification of critical infrastructure, and the implementation of a holistic multilayered approach to cybersecurity. This approach should ensure that a successful attack on one layer does not compromise other layers of the system and/or lead to loss of safety, security or continuity of critical functions. The system should also adopt a continuous improvement approach to ensure that necessary enhancements to planned technical or procedural evolutions are coordinated, implemented, and kept up to date.

3.2 Ensure civil aviation is cyber-resilient

A cyber-resilient civil aviation system is a system that, under attack, can maintain its critical functionalities: i.e., supports safe and secure flight operations with minimal, if any, disruption. The system should also include appropriate cooperation and information-sharing mechanisms between aviation stakeholders, such as government, industry and, where appropriate, with civil law enforcement and military authorities.

3.3 Ensure civil aviation is self-strengthening by adopting a "Security by Design" approach

Adopting a security by design approach for civil aviation requires, at the outset of a system's conception, consideration of security objectives that need to be achieved during a system's design process, along with traditional operational and safety objectives. Ensuring the security of critical elements and processes "by design" changes the security paradigm from reactive to proactive, and fosters the development

[1] https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx
[2] ICAO State letter 2020/114

of a self-protected civil aviation system, therefore enabling it to evolve and enabling improved security and resilience.

3.4 Ensure coordination of aviation cybersecurity within civil aviation and with concerned non-aviation stakeholders

In order to ensure a consistent and complimentary approach to aviation cybersecurity across aviation disciplines, the civil aviation system must ensure the comprehensive management of cyber risks to civil aviation by coordinating the safety and security aspects of aviation cybersecurity. In addition, coordination of aviation cybersecurity should extend beyond civil aviation to other concerned entities such as national/regional/international cybersecurity authorities, law enforcement, military, etc.

4. Elements of the Cybersecurity Policy

This section provides guidance on the elements included in the model Cybersecurity Policy in Appendix A. It is therefore recommended to be read together with the model Cybersecurity Policy.

4.1 Governance and Organization

4.1.1 States should designate an Appropriate Authority for Aviation Cybersecurity (AA/Cyber) with an overall mandate and responsibility for aviation cybersecurity and cyber resilience.

4.1.2 There is no one-size-fits-all model as to where the AA/Cyber would fit within individual States' civil aviation organizational structures. The decision would be impacted by several considerations related to the national aviation and relevant non-aviation set-up in terms of entities and mandates. It is important however that the AA/Cyber be provided with the required resources and authority to be able to discharge its mandate, including the negotiation and coordination with non-aviation concerned stakeholders.

4.1.3 Overall, the designated AA/Cyber should:

- determine, in coordination with the national competent authority for cybersecurity, the roles and responsibilities to be undertaken by each authority;
- lead the development of aviation cybersecurity regulations;
- clearly define roles and responsibilities for the different civil aviation domains within the national competent authority for civil aviation;
- coordinate the definition of roles and responsibilities of civil aviation entities overseen by the national competent authority for civil aviation through the national safety and security programmes;
- define the elements of civil aviation cybersecurity culture and monitor its implementation;
- define regulations, processes, requirements, and roles for cybersecurity crisis management, including testing requirements and frequencies; and
- coordinate cross-cutting aviation cybersecurity issues with relevant non-aviation stakeholders involved in aviation cybersecurity such as information sharing and incident investigation.

4.2 Risk Management

4.2.1 Managing cybersecurity risks should draw on aviation safety and security risk management frameworks in order to develop an integrated and accurate assessment of cybersecurity threats and risks, and ensure the development and implementation of effective mitigation measures that take into account safety requirements and the implications of mitigation measures on safety and continuity of civil aviation.

4.2.2 All data and systems should have identified ownership at all times. Identifying and maintaining ownership establishes accountabilities and supports the management of data and systems from adoption to disposal. As such, rules and processes should be established by the owners to include physical locations of data and systems, access rights, management rights, and security requirements based on data and system classification. This will eventually support adequate usage of data and systems by the right people, setting and implementing quality control standards, and resolve issues and conflicts.

4.3 Critical Systems Security

4.3.1 Defence in depth principles should be applied to protect critical systems. Defence in depth integrates people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization[3]. It is an approach to cybersecurity in which a series of defensive mechanisms are layered in order to protect critical systems, data and information. This multilayered approach with intentional redundancies increases the security of a system as a whole and addresses many different attack vectors[4].

4.3.2 The AA/Cyber should ensure that civil aviation entities identify and adequately protect their critical systems as well as develop the ability to detect, respond to, and recover from cyber incidents.

4.4 Data Security

4.4.1 Periodic offline secure backup of critical data should be considered as an enabler to support information availability and integrity. It is however paramount to develop a robust backup policy, in line with risk assessments, since an offline backup taken while a cyber-attack is in progress would be already compromised and therefore cannot be used to restore access to critical information.

4.4.2 Encryption of sensitive data should be considered as an enabler to support information confidentiality. It is however important to define, in line with risk assessments, processes for the use of encryption that strike the appropriate balance between the level of confidentiality and operational performance requirements, especially for "live" data required for flight safety, as well as taking into account the resources needed to manage the data.

4.4.3 Processes should be established to ensure continuity of critical functions in case of loss of data availability and/or integrity.

4.5 Supply Chain Security

4.5.1 Entities should ensure that software and hardware used in critical aviation functions comply with cybersecurity requirements throughout the life cycle of aviation systems, from design and development through operation and maintenance, continuing through the safe and secure disposal.

4.5.2 Service Level Agreements can be leveraged to include cybersecurity requirements for hardware and software as well as for the update, upgrade, and patching in case of discovered vulnerabilities.

---

[3] NIST Special Publication 800-53 Rev.5: https://doi.org/10.6028/NIST.SP.800-53r5

[4] Defence in depth is commonly referred to as the "castle approach" because it mirrors the layered defences of a medieval castle, where in order to penetrate a castle attackers are faced with the moat, draw-bridge, rampart, towers, etc.

4.6 **Physical Security**

4.6.1 Examples of physical security controls of relevance to aviation cybersecurity include, inter alia, defining physical access management and control policies, background checks of personnel with administrative rights on systems/databases, or with access to sensitive and/or critical data, recommendations for separation of duties and/or rotation in personnel with access to, or ability to modify critical systems, etc.

4.7 **Information, Communication, Technology (ICT) Security**

4.7.1 Examples of ICT security controls of relevance to aviation cybersecurity include, inter alia, access control policies and application of least privilege principles, software/hardware firewalls and network security, cryptography, organizational password policies, end-point protection, network monitoring and detection of anomalies, network separation, device management, etc.

4.8 **Incident Management and Continuity of Critical Functions**

4.8.1 The AA/Cyber should define regulations, processes, requirements, and roles for cyber incidents management, recovery and continuity of critical systems.

4.8.2 Existing crisis management and business continuity plans should be leveraged to include response to and recovery from cyber incidents.

4.8.3 Testing emergency response and business continuity plans should be periodically conducted with the aim to improve the plans as well as the capabilities of responders. Testing should include all relevant stakeholders and comprise a combination of Table Top Exercises (TTX) as well as live tests.

4.9 **Cybersecurity Culture**

4.9.1 Cybersecurity culture should be implemented across all aviation entities.

4.9.2 Cybersecurity culture should be endorsed by organizational leadership, and should include a programme to be undertaken by all personnel.

4.9.3 The programme should include recurrent cybersecurity education (including principles of cyber hygiene practices), awareness on latest threats, training, and testing (both as part of training and live simulation of attacks) to assess the level of cyber awareness/hygiene.

4.9.4 Cybersecurity culture should include elements from safety and security cultures, e.g. self-reporting, reporting of suspicious behaviour/practice, just culture, etc.

— — — — — — — —

Appendix A

Model Cybersecurity Policy

1. Introduction

1.1 This cybersecurity policy shall be the framework for further development and implementation of aviation cybersecurity. It shall be published, disseminated to relevant stakeholders, and periodically reviewed.

1.2 Further guidance material shall be developed to support the implementation of this cybersecurity policy.

2. Scope

2.1 Aviation cybersecurity shall address the security and resilience of the civil aviation system, as well as support the collaboration with concerned non-aviation entities and authorities, including national cybersecurity authority, national security, law enforcement and military, as appropriate.

2.2 Aviation cybersecurity shall be coordinated at the national level with aviation safety, aviation security, critical infrastructure protection, cyber defence and military.

2.3 Aviation cybersecurity shall be coordinated at the international level with equivalent Foreign Appropriate Authorities designated for Aviation cybersecurity.

3. Objectives

3.1 The overall objectives of this aviation cybersecurity policy are to ensure the security, resilience, and self-strengthening of the civil aviation system against cyber threats and risks, and to ensure the coordination of aviation cybersecurity with concerned national authorities and entities.

4. Governance and Organization

4.1 In accordance with [Regulation/Legislation Reference for the designation], [Entity Name] shall be the Appropriate Authority for Aviation Cybersecurity (AA/Cyber) with an overall mandate for aviation cybersecurity and cyber resilience.

4.2 The AA/Cyber shall:

- engage with the national competent authority for cybersecurity in order to define the civil aviation cybersecurity roles and responsibilities to be undertaken by each authority;
- coordinate and contribute to the development of aviation cybersecurity regulations;
- define, coordinate, and provide support to aviation safety and aviation security appropriate authorities to include aviation cybersecurity requirements, including oversight and quality control elements, in the national State Safety Programme (SSP) and the National Civil Aviation Security Programme (NCASP);
- define, support, and monitor the implementation of the cybersecurity culture programme by all civil aviation stakeholders;
- define regulations, processes, requirements, and roles for cybersecurity crisis management; and
- coordinate cross-cutting aviation cybersecurity issues with relevant non-aviation stakeholders involved in aviation cybersecurity.

5. Risk Management

5.1 Cybersecurity shall be intelligence driven, threat based and risk managed.

5.2 Risk management shall be an integral part of overall systems' life cycle.

5.3 All data and systems shall have identified ownership at all times.

6. Critical Systems Security

6.1 Critical functions, systems, and infrastructure shall be identified through risk management processes.

6.2 Security by design approach, coupled with Defence in depth principles, shall be applied to protect critical systems.

6.3 Redundancy of critical systems shall be considered as an enabler for system security.

7. Data Security

7.1 Data and information shall be protected during storage and transmission, in line with its sensitivity profile.

8. Supply Chain Security

8.1 End-to-end management of software/hardware supply chain shall be part of aviation cybersecurity management.

8.2 Software and hardware used in critical aviation functions shall comply with cybersecurity requirements throughout the life cycle of aviation systems.

9. Physical Security

9.1 Physical security (including personnel security) shall be part of aviation cybersecurity management.

9.2 Physical security shall safeguard people, infrastructure, facilities, equipment, material, and documents from unlawful interference and protect critical aviation systems from unauthorized physical access.

9.3 Physical security shall contribute to risk management through supporting the identification of threat actors and/or the likelihood of attacks on civil aviation critical infrastructure.

10. Information, Communication, Technology (ICT) Security

10.1 ICT security shall be part of aviation cybersecurity management.

10.2 ICT security shall define and implement logical security measures as well as contribute to cyber incident management, recovery, and operation continuity processes.

10.3 ICT security shall contribute to risk management through the identification of vulnerabilities, attack vectors, and monitoring the evolution of the aviation cybersecurity threat landscape.

11. Incident Management and Continuity of Critical Functions

11.1 Safety of operations and continuity of critical functions shall be the main drivers in incident management processes.

11.2 Testing crisis management and recovery plans shall be an integral part of incident management.

12. Cybersecurity Culture

12.1 An education, awareness, training, and exercise plan shall be an integral part of aviation cybersecurity management.

12.2 Cybersecurity culture shall be fully coordinated with existing safety and security cultures.

12.3 Cybersecurity culture shall be supported by robust internal and, to the extent possible, external information sharing practices.

APPENDIX C

ICAO

Security and Facilitation Strategic Objective

Aviation Cybersecurity Strategy

October, 2019

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO

Security and Facilitation Strategic Objective

Aviation Cybersecurity Strategy

October, 2019

Approved by and published under the authority of the Secretary General

INTERNATIONAL CIVIL AVIATION ORGANIZATION

Published in separate English, Arabic, Chinese, French, Russian
and Spanish editions by the
INTERNATIONAL CIVIL AVIATION ORGANIZATION
999 Robert-Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

For ordering information and for a complete listing of sales agents
and booksellers, please go to the ICAO website at www.icao.int

Aviation Cybersecurity Strategy
https://www.icao.int/cybersecurity/Pages/Cybersecurity-Strategy.aspx

AVIATION CYBERSECURITY STRATEGY

THE VISION OF A GLOBAL AVIATION CYBERSECURITY STRATEGY

The civil aviation sector is increasingly reliant on the availability of information and communications technology systems, as well as on the integrity and confidentiality of data. The threat posed by possible cyber incidents to civil aviation is continuously evolving, with threat actors focusing on malicious intents, disruptions of business continuity and the theft of information for political, financial or other motivations.

Recognizing the multi-faceted and multi-disciplinary nature of cybersecurity, and noting that cyber-attacks can simultaneously affect a wide range of areas and spread rapidly, it is imperative to develop a common vision and define a global Cybersecurity Strategy.

ICAO's vision for global cybersecurity is that the civil aviation sector is resilient to cyber-attacks and remains safe and trusted globally, whilst continuing to innovate and grow.

This can be achieved through:

- Member States recognizing their obligations under the *Convention on International Civil Aviation* (Chicago Convention) to ensure the safety, security and continuity of civil aviation, taking into account cybersecurity;

- coordination of aviation cybersecurity among State authorities to ensure effective and efficient global management of cybersecurity risks, and

- all civil aviation stakeholders committing to further develop cyber resilience, protecting against cyber-attacks that might impact the safety, security and continuity of the air transport system.

The Strategy aligns with other cyber-related ICAO initiatives, and coordinated with corresponding safety and security management provisions. The Strategy's aims will be achieved through a series of principles, measures and actions contained in a framework built 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. INTERNATIONAL COOPERATION

1.1 Cybersecurity and aviation are both borderless in nature. Both require cooperation at the national and international level and call for a mutual recognition of efforts to develop, maintain and improve cybersecurity with the aim to protect the civil aviation sector from all cyber threats to safety and security.

1.2 Aviation cybersecurity needs to be harmonized at the global, regional and national levels in order to promote global coherence and to ensure full interoperability of protection measures and risk management systems.

1.3 ICAO is the appropriate global forum to engage States in addressing cybersecurity in international civil aviation. To this end, ICAO will organize, facilitate and promote international events that serve as a platform for knowledge exchange between States, international organizations and industry. States are encouraged to engage in discussions on cybersecurity in civil aviation.

2. GOVERNANCE

2.1 All ICAO Member States are encouraged to support and build upon the ICAO Aviation Cybersecurity Strategy, to ensure the safety, security and continuity of civil aviation in a world increasingly jeopardized by cybersecurity threats.

2.2 States are encouraged to develop clear national governance and accountability for civil aviation cybersecurity. Civil Aviation authorities are encouraged to ensure coordination with their competent national authority for cybersecurity, recognizing that the overall cybersecurity authority for all sectors may reside outside the responsibility of the civil aviation authority. It is also essential that appropriate coordination channels among various State authorities and industry stakeholders be established.

2.3 Furthermore, Member States are encouraged to include cybersecurity in their national civil aviation safety and security programmes. To this end, ICAO should also include cybersecurity in regional and global plans and work towards a common baseline for cybersecurity Standards and Recommended Practices (SARPs).

3. EFFECTIVE LEGISLATION AND REGULATION

3.1 The principal aim of international, regional and national legislation and regulation on cybersecurity for civil aviation is to support the implementation of a comprehensive Cybersecurity Strategy to protect civil aviation and the travelling public from the effects of cyber-attacks.

3.2 Member States must ensure that appropriate legislation and regulations are formulated and applied, in accordance with ICAO provisions, prior to implementing a national cybersecurity policy for civil aviation. Further development of appropriate guidance for States and industry in implementing cybersecurity related provisions is necessary. To this end, ICAO is committed to create, review and amend, as appropriate, guidance material relating to the inclusion of cybersecurity aspects to security and safety.

3.3 Relevant international legal instruments should be analysed to identify existing or missing key legal provisions in air law for the prevention, prosecution, and timely reaction to cyber-incidents in order to form the basis for consistent and coherent implementation of cybersecurity legislation and regulations throughout the global aviation sector. In the meantime, States are encouraged to ratify ICAO instruments, including the *Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation* (Beijing Convention) and *Protocol Supplementary to the Convention for the Suppression of Unlawful Seizure of Aircraft* (Beijing Protocol).

3.4 States are encouraged to consider whether their national legislation requires an update or the adoption of new national legislation to allow for the prosecution of terrorist-related cyber threats as well as cyber-attacks negatively impacting civil aviation. In parallel, States are encouraged to set up appropriate mechanisms for cooperation with 'good faith' security research, which is research activity carried out in an environment designed to avoid affecting the safety, security and continuity of civil aviation.

4. CYBERSECURITY POLICY

4.1 Cybersecurity is to be included within a State's aviation security and safety oversight systems as part of a comprehensive risk management framework.

4.2 Recognizing there are different risk assessment methodologies, priority should be afforded to the amendment and possible development of guidance material related to cybersecurity threat and risk assessments, with the aim to achieve comparability of the outcomes of such assessments.

4.3 Across the civil aviation sector, cybersecurity policies may consider the complete life-cycle of the aviation system, and include elements such as: cybersecurity culture, promotion of security by design, supply chain security for software and hardware, data integrity, appropriate access control, pro-active vulnerability management, improving agility in security updates without compromising safety, as well as incorporating systems and processes to monitor cybersecurity relevant data.

5. INFORMATION SHARING

5.1 The civil aviation sector is a global, interdependent system with many common systems and cyber-attacks can easily spread and have global impact. The objective of information sharing is to allow for prevention, early detection and mitigation of relevant cybersecurity events before they lead to wider effects on aviation safety or security. A culture of information sharing will significantly reduce systemic cyber risk across the aviation sector, the value of which has already been proved across aviation safety and security.

5.2 The sharing of information on such aspects as vulnerabilities, threats, events and best practices, through established and trusted relations can reduce the impact of ongoing attacks. Appropriate information sharing mechanisms must be recognized, in line with existing ICAO provisions.

6. INCIDENT MANAGEMENT AND EMERGENCY PLANNING

6.1 There is a need, in line with existing incident management mechanisms, to have appropriate and scalable plans that provide for the continuity of air transport during cyber incidents. It is recommended that States and the aviation sector make use of existing contingency plans that are already developed and amend these to include provisions for cybersecurity.

6.2 Cybersecurity exercises are a useful tool to test existing cyber resilience and identify improvements, and are therefore highly encouraged. Such exercises can follow different formats (such as table-top exercises, simulations, or real-time exercises) and also vary in scale, (international, national, organizational).

7. CAPACITY BUILDING, TRAINING AND CYBERSECURITY CULTURE

7.1 The human element is at the core of cybersecurity. It is critically important that the civil aviation sector takes tangible steps to increase the number of personnel that are qualified and knowledgeable in both aviation and cybersecurity. This can be done by increasing awareness of cybersecurity, as well as education, recruitment and training. Curricula relevant to cybersecurity, and – where practical – aviation-specific cybersecurity at all levels should be included in the national educational framework as well as in relevant international training programmes. Innovative ways to merge and crosslink traditional information technology and cyber career paths with aviation relevant professionals should be pursued.

7.2 The support and stimulation of skills development in the existing and new workforce should lead to the fostering of cybersecurity innovation and appropriate research and design in the aviation sector. Appropriate job-related training should be provided on a continuous basis to support personnel in their daily roles.

7.3 Cybersecurity could be included in the strategy for the next generation of aviation professionals as ICAO is well-placed to work with States and industry to develop role-based competency requirements for aviation professionals.

7.4 The civil aviation sector has established an enviable safety record which is founded upon a pro-active safety culture which is seen as everybody's responsibility. The principles of this safety culture are to be applied to develop and maintain a cybersecurity culture across the aviation sector.

— END —

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