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.

— END —