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 —