Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE ESTUDIO

NACC/DCA/12 — WP/17
21/06/24

Twelfth Meeting of Directors of Civil Aviation of North America, Central America and the Caribbean (NACC/DCA/12)

Placenta, Belize 09-11 July 2024

Agenda Item 3: Aviation Security (AVSEC) and Facilitation (FAL)

INITIATIVE FOR THE PROTECTION OF CRITICAL INFORMATION, COMMUNICATIONS TECHNOLOGY SYSTEMS AND RELATED CRITICAL DATA USED TO PROTECT CIVIL AVIATION FROM ILLEGAL AERONAUTICAL INTERFERENCE IN COCESNA MEMBER STATES

(Presented by Belize, Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua)

EXECUTIVE SUMMARY

This Working Paper presents the COCESNA initiative on cybersecurity to support and guide the Civil Aviation Authorities of the Member States in the establishment of policies and implementation of measures for the protection of critical information technology systems and aeronautical communications. In addition to guiding aviation industry operators for their identification and protection; including airports, aircraft operators, ATS providers, communication service providers, and ground handling agents, among others.

To promote a common interpretation among States on cyber threats, risks, and the formulation of criteria; to strengthen aviation security and facilitation.

Action:	Suggested actions are presented in Section 6.
Strategic Objectives:	• Security & Facilitation
References:	• ICAO Annex 17 • Doc.8973 ICAO • Chapter 18 of the Aviation Security Manual (Doc 8973 – Restricted) • Air Traffic Management Safety Manual (Doc 9985 – Restricted) • Guidance on cybersecurity policy and Cybersecurity Culture in civil aviation.

1. Introduction

1.1 In the current context of civil aviation, air traffic is expected to increase in the long term, technology will continue to evolve rapidly, operations will become increasingly complex, and, consequently, operational conditions will become more difficult. Rapid technological changes are altering how civil aviation works and making the system more vulnerable to cybersecurity threats. Malicious cyber activities can impact civil aviation in various ways, from brief disruption of operations to catastrophic consequences. Risks are increasing rapidly, so a sustainable cybersecurity framework is urgently needed at the international, regional, and national levels.

1.2 The creation of a solid cybersecurity infrastructure, supported by close cooperation between States and industry, allows the creation of a common awareness of cybersecurity that ultimately leads to a safer and more resilient civil aviation system.

1.3 As part of the commitment to the protection of security of its Member States, COCESNA, through its different managements: Central American Agency for Aeronautical Safety, Central American Air Navigation Agency, Information Technology and in coordination with the AVSEC Regional Group of Central America, made up of AVSEC specialists from the Central American region, considering the importance of the provisions of Annex 17 to the Convention on International Civil Aviation, in particular Standard 4.9.1 where information technology systems are identified and critical communications and data that are used for civil aviation, and that based on a risk assessment, develop and implement the corresponding measures to protect them from illicit interference, carried out the task of putting into practice the initiative for the identification, risk assessment and protection of critical information technology systems, communications and related critical data used operationally in civil aviation and that may be subject to unlawful aeronautical interference in COCESNA Member States.

2. Discussion

2.1 Cybersecurity is not a new concept in the field of civil aviation. However, as cybersecurity threats have become increasingly frequent, it has become one of the central elements of discussions and analyses of risks and vulnerabilities of the civil aviation system. The civil aviation sector is particularly at risk because cyber-attacks are more likely to thrive in a sector whose components are growing interdependently functionally and digitally, and also because the cyber defence mechanisms currently used by the sector of civil aviation are not yet adequate to address this persistent and adaptive threat.

2.2 Given the multifaceted and multidisciplinary nature of cybersecurity and given that cyberattacks can simultaneously affect a wide range of areas and spread quickly, it is imperative to devise a common vision and define a cybersecurity strategy. This can be achieved by:

- recognition by States of their obligations under the Convention on International Civil Aviation (Chicago Convention) to ensure safety and security and continuity of civil aviation, including cybersecurity;

- coordination of aviation cybersecurity between State authorities to ensure effective and efficient management of cybersecurity risks on a global scale; and

- the commitment of all aviation stakeholders to deepen aviation resilience and protect against cyber-attacks that could affect safety, aviation security, and the continuity of the air transport system.

2.3 Considering that in terms of cybersecurity COCESNA began with the establishment of a Specific Objective within the Strategic Plan aimed at "Implementing Cybersecurity following good practices in the aeronautical and technological sector", and through which it has managed to establish initiatives that range from a regulatory framework, socialization, implementation of protection measures and cybersecurity groups and in support of the detection of specific cybersecurity needs identified through technical assistance in aviation security, carried out in its Member States, and uniting efforts to begin this initiative taking as reference the initiatives implemented internally.

2.4 The actions that are carried out and that are part of the implementation of minimum measures of this Central American regional initiative for the security and protection of civil aviation operations, within the Member States Belize, Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua are:

a) protection of systems and data against unauthorized access, modification and use;
b) control over lack of availability and integrity due to failures in program compilation computer problems and/or misuse of configurations;
c) reduction of improper manipulation of systems and their data.

3. Developments

3.1 Given the growing importance of cybersecurity and the need to protect the aviation system against new threats in the Central American States and within the framework of the EU – Latin America and the Caribbean Aviation Association (EU-LAC APP) project, coordinated a meeting with the European Union Aviation Safety Agency (EASA) where he offered an overview of the European approach to cybersecurity, the ability to provide cybersecurity training and the exchange of experiences with COCESNA.

3.2 In addition, areas of mutual interest and future cooperation in aviation cybersecurity risk management were identified.

4. Roadmap

4.1 Identification of information, communication, and data systems identified as critical from an aviation safety perspective:

4.2 As part of the beginning of the process of mitigating illicit interference in the aviation industry, Member States are recommended that cybersecurity risks be identified and evaluated, considering all possible consequences of an attack on the civil aviation system for example: protection, security, efficiency, continuity of service, etc.; as well as the possible sources of threats and vulnerabilities that may exist.

4.3 In addition, it is recommended that the identification and evaluation of cybersecurity risks be coordinated and carried out by a group of experts in cyber and civil aviation, if possible, with experience in cybersecurity and should be able to identify their systems of information, communication, and data that can be identified as critical, this to delimit the scope and capacity of the State at the time its systems are threatened, and thus be able to better manage a threat in the area of cybersecurity.

4.4 To this end, we have proposed a format that allows for the identification of critical information, communication, and data systems according to the State.

COCESNA MEMBER STATES Belize, Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua			
Government entities	Airport operators	Air operators	Industry in general

4.5 Development of a specific risk assessment for the identified critical systems. Analysis of possible threats and vulnerabilities, considering both technological and human factors (considering that IT Management already has an internal risk analysis, this could be replicated in the CA region, with support from the authorities' IT staff of Civil Aviation and other relevant entities, if they exist). It could start with Guatemala and Honduras.

Risk assessment

4.6 As part of a risk assessment process, Member States should, through their respective designated authorities and as a matter of national cybersecurity policy, work with qualified personnel to conduct continuous assessments of the vulnerability and interdependence of their systems, and thus establish measures to mitigate potential cyberattacks and verify the implementation of such measures as part of their regular compliance monitoring activities (e.g. inspections and audits).

4.7 Within these evaluations, Member States, with the support of national civil aviation authorities, must carry out these evaluations under a methodology that considers the main risk components:

1. Threat scenario: the identification and possible description of an unlawful act of interference and the methods to carry out the said act, the national authorities of the States must create a scenario that is as real as possible.

2. Probability of attack: States must review the probability of an attack occurring on aviation cyber systems, without excluding any of them, no matter how complex they may seem.

3. Consequences: in the event of a cyber-attack on aviation systems, what is the magnitude and the effects that may have repercussions (human, economic, and political)?

4. Vulnerability: States must be able to self-identify their existing vulnerabilities in terms of the magnitude of a cyber-attack.

5. Residual risk: Once the probability, consequences, and vulnerability have been analysed, the risk that may persist even when taking measures according to these variables.

4.8 Once States and their national civil aviation authorities carry out this risk assessment, it is important to establish minimum criteria for the protection of information and communication technology systems and related critical data used to protect civil aviation from illicit interference that must be implemented by each of the States and their civil aviation authorities.

4.9 Cybersecurity infrastructure: It is related to the technical administration of cybersecurity devices and tools, such as (without being limiting):

- Antivirus;
- Antispam;
- Firewall;
- Web Application Firewall (WAF);
- Vulnerability scanning;
- Video surveillance;
- Remote support;
- Data encryption;
- Secure erase.

4.10 IT asset management: Related to the administration of technological equipment and devices that includes:

- Life cycle of IT assets (Planning, provision, administration, discharge);
- IT asset classification;
- Identification of critical assets;
- Hardware Inventory;
- Inventory and assignment of Software licenses;
- Patch management

5. Conclusion

5.1 The protection of critical information technology, communications, and data systems in civil aviation is essential to ensure safety and operational efficiency. The implementation of robust cybersecurity measures, encryption protocols, and continuous monitoring systems are essential to prevent threats and ensure the integrity of information in this highly sensitive sector. Collaboration between government entities, aeronautical entities, and cybersecurity experts is key to maintaining a safe and reliable air environment.

5.2 Aviation security, as a fundamental basis for the growth and sustainability of the aviation industry, requires the integration of harmonized measures applied by Member States, where the exchange of knowledge and experiences that allow the execution of good practices and standardized improvement opportunities to raise compliance levels and give recognition to the Central American region as a promoter of actions in the field of aviation security, which guide to guarantee the protection of civil aviation against acts of unlawful interference through technological means that may affect your critical information, communications and data systems.

6. Suggested actions

6.1 The Meeting is invited to:

a) take into consideration the initiatives undertaken by COCESNA Member States for the implementation of cybersecurity at the regional level;

b) encourage States and organizations on the development of initiatives, establishment of measures, development of plans that promote the protection of critical information technology systems, communications and related critical data used, to protect civil aviation from interference aeronautical illegalities; and

c) promote the sharing of lessons learned, and the benefits obtained with their implementations for the benefit of other States and organizations.

— END —