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

WORKING PAPER

NACC/WG/6 — WP/23
20/08/21

Sixth North American, Central American and Caribbean Working Group Meeting (NACC/WG/6)
On-line, 25 to 27 August 2021, 09:00 to 13:00 (UTC-5)

Agenda Item 4: Implementation of Air Navigation Issues
4.8 Emerging technologies and new regional challenges

CANSO – AIRBUS AIR TRAFFIC MANAGEMENT CYBERSECURITY POLICY TEMPLATE INTRODUCTION

(Presented by CANSO)

EXECUTIVE SUMMARY	
Cyber-attacks are a growing threat worldwide because of increased digitalization and the interconnectivity of systems. Civil aviation is particularly sensitive to this emerging threat due to its widely interconnected systems. Any disruption of systems due to a cyber-attack can seriously affect the safety and security of flights and the reputation of civil aviation in the public eye. As such, ICAO addressed this emerging threat to civil aviation through ICAO resolution A40-10 Addressing Cybersecurity in Civil Aviation.	
Action:	Suggested actions are presented in Section 4.
Strategic Objectives:	• Air Navigation Capacity and Efficiency • Economic Development of Air Transport
References:	• ICAO Assembly Resolution A40/10 Addressing Cybersecurity in Civil Aviation • ICAO Document 9985 – ATM Security Manual • ICAO Aviation Cyber Security Strategy • ICAO – CANSO – Airbus Air Traffic Management Cybersecurity Policy Template

1. Introduction

1.1 The increase of sharing information and common situational awareness across the aviation industry means greater potential exposure to cyber-attack. The threat is genuine, serious, and civil aviation must develop and execute security strategies and plans to ensure continued mission operations regardless of the threat. Cyber threats are continually evolving and becoming increasingly sophisticated. As civil aviation moves towards open standards and systems, it needs to become more proactive and prepared to mitigate the threat.

1.2 The aviation community need to recognize, act, control, recover and learn for future occurrences and find solutions to protect the aviation system while at the same time preparing for and minimizing the possibility of a cyber-attack.

1.3 All aviation stakeholders; States, and industries need to counter cyber threats to civil aviation and implement a cybersecurity strategy to avoid cyber-attack and ensure business continuity

2. Discussion

2.1 It is vital that the civil aviation sector integrates cybersecurity policies as part of its standard procedures and integrates them in every part of its aviation system. Aeronautical systems are vulnerable to cyber threats, for example, IT sabotage, data corruption and availability (notable ransomware), software corruption, communication disruption or interruption, satellite communication interference, cyber-attack, systems sabotage, data breaches and 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. Also, it impacts productivity, business continuity and the financial health of the organization.

2.2 Civil Aviation Authorities and ANSPs 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 level of safety.

2.3 To protect their operation from internal and external threats, States should implement cybersecurity mechanisms across the ATM system. Cybersecurity should be in the security culture through the training of air transport personnel (ANSPs, airlines, airports and others that have a direct and indirect relationship with ATM operations). Applying good basic practices introduced in training, workshops, and seminars can reduce the cyber-attacks probability, affecting public confidence, although representing a minimal security risk.

2.4 Civil Aviation Authorities actively cooperates with all stakeholders to establish national and international mechanisms to systematically share cyber threats, incidents, trends, and mitigation efforts.

2.5 To integrate cybersecurity as part of a risk management process, combine risk identification and analysis, action, and measure to avoid cyberattacks.

3. Development

3.1 In assisting the aviation community, ICAO, CANSO, and Airbus developed the first of its kind Air Traffic Management Cybersecurity Policy Template. The policy helps ensure the resilience of the aviation system by outlining steps for creating a custom fit solution for individual organizations seeking to establish cybersecurity policies as part of their standard procedures and integrate them into every aspect of their business.

3.2 The Air Traffic Management Cybersecurity Policy Template covers all aviation stakeholders' functional structure, ensuring cybersecurity procedures and practices in all services under the State oversight.

3.3 ICAO, CANSO, and Airbus organized a series of events addressed to States and ANSPs to support the development of individual cybersecurity policy. The first event was the Introduction to Cybersecurity and covered the cybersecurity strategy, information to understand the threats and risks associated with a cyber-attack and examples of a security breach within our industry. The objective of the second event concentrated on explaining the ATM Cybersecurity Policy Template, support States and ANSPs to measure their cybersecurity implementation status and start with the development of the cybersecurity policy.

3.4 Following the events, ICAO, CANSO, and Airbus developed a more direct approach to assist every State and ANSP to prepare their own Air Navigation Service – Cybersecurity Manual policy. Also, a checklist was created and shared with the States, and ANSPs aimed to measure all of the requirements on cybersecurity implementation explained in the ATM Cybersecurity Policy Template.

3.5 ICAO, CANSO, and Airbus support Cuba, El Salvador, and COCESNA to evaluate their cybersecurity maturity level. States and ANSPs are submitting their information and completing the checklist for evaluation.

3.6 The different activities developed under the ICAO-CANSO-AIRBUS initiative will allow States to lay the groundwork for developing cyber-protection measures, business continuity, and maturity during the implementation process to increase State and Regional security.

4. Suggested actions

4.1 The Meeting is invited to:

a) Take note of the information provided in the working paper;
b) encourage States and ANSPs to develop their cybersecurity and strategic plan to ensure continued mission operations regardless of the cyber threat; and
c) participate in cybersecurity assessment and evaluation

— END —