59th CONFERENCE OF DIRECTORS GENERAL OF CIVIL AVIATION ASIA AND PACIFIC REGIONS

Cebu, Philippines
14 to 18 October 2024

AGENDA ITEM 5: AVIATION SECURITY AND FACILITATION

INTEGRATION OF CYBER SECURITY IN USAP CMA AS A SEPARATE CRITICAL ELEMENT

(Presented by Pakistan)

INFORMATION PAPER

SUMMARY

In the few years there has been a notable rise in the use of Information and Communication Technology (ICT) tools within aviation infrastructure resulting in heightened concerns regarding cyber security. The increasing frequency and severity of cyber-attacks targeting civil aviation systems highlights the need for enhanced protective measures. This article explores the significance of integrating cyber security protocols into evaluations of the USAP CMA. Suggests incorporating cyber security as an independent Critical Element due to the impact of cyber threats on Civil Aviation, during USAP CMA Audits.

INTEGRATION OF CYBER SECURITY IN USAP CMA AS A SEPARATE CRITICAL ELEMENT

1. INTRODUCTION

1.1. There has been a growing wave of cyber-attacks on the aviation sector, compromising on systems safety, integrity, and confidentiality. It thus becomes very imperative that comprehensive cybersecurity measures are integrated into existing audit frameworks in aviation systems, most of which have been digitalized. This paper looks into the USAP-CMA current audit program with an emphasis on specific cybersecurity requirements that need to be included as a matter of necessity in its audit processes

1.2. In the previous years, cybersecurity attacks on critical infrastructures across the world have increased and cause financial costs and operations. For example, in 2023, the FBI Internet Crime Complaint Center received 880,418 cyber incidents that led to a huge financial loss of $12.5 billion, the highest of the past five years. Of note, ransomware attacks increasingly targeted organizations within critical infrastructure sectors, with more than two in five of such attacks reported to the FBI in 2023 involving such sectors. The upward pattern of both frequency and costs of cybercrimes is indicative of significant risks for the stability and security of key services and infrastructure **(Insurance Information Institute, 2024; Cybersecurity Dive, 2024)**

1.3. Estimating exact losses on account of cybercrime-related attacks is difficult because of a lack of publicly available information, documentation, and published incident reports. There are few disclosures relating to the financial implications of cybercrime for industries regarding compensation paid to victims and ransom payments during ransomware attacks. Apart from this, other significant indicators include the number of entities shutdown, such as airports and the incurred number of lost operational hours, both lag in reporting. This kind of transparency is a lack of other important factors that make it difficult to assess the real economic and operational costs arising from cybercrime.

2. DISCUSSION

2.1 Specific requirements for Cyber Security in USAP-CMA Audits

The USAP-CMA currently focuses on evaluating Member States' capabilities to implement Annex 17 and Annex 9 standards. However, with the increased incidence of cyber threats, it is imperative to expand the scope to include cyber security as a separate Critical Element rather be related to specific protocol questions.

2.2 Competencies for USAP-CMA Auditors in Cyber Security

To effectively audit cyber security requirements, USAP-CMA auditors should possess specific competencies related to cyber security standards and frameworks. According to Doc 9807 – USAP CMA Chapter 6.5 the competencies listed for a USAP CMA Auditor are as below:

> *"6.5.2 TMs are expected to have:*
> *a) recent work experience with an appropriate authority as an aviation security inspector in any one of the*
> *following audit areas pertaining to USAP-CMA:*
>
> *1) OPS;*
> *2) IFS;*
> *3) PAX; and*
> *4) CGO.*

These competencies should include:

- **Working Knowledge of Cyber Security Standards and Frameworks**: Auditors must be familiar with internationally recognized cyber security standards such as ISO/IEC 27001, NIST Cybersecurity Framework, and other relevant frameworks. This knowledge will enable them to assess the adequacy of cyber security measures implemented by Member States.
- **Understanding of Cyber Security Risk Management**: Auditors should be equipped with skills to evaluate risk management processes related to cyber security, including identifying, assessing, and mitigating risks associated with cyber threats in aviation operations.
- **Experience in Cyber Security Auditing Practices**: Practical experience in auditing cyber security practices, particularly in critical infrastructure sectors like aviation, is essential for auditors to accurately identify weaknesses and recommend effective countermeasures.

2.3 Proposal for Integration of Cyber Security in USAP-CMA

To address these challenges, it is recommended that the ICAO consider revising the USAP-CMA framework to incorporate the following:

- **Specific Requirements for Cyber Security**: Define clear cyber security requirements that Member States must adhere to, considering the unique vulnerabilities in aviation.
- **Inclusion of Cyber Security as a Critical Element**: Treat cyber security as a standalone Critical Element within the USAP-CMA based on the SARP's stated in Annex 17 and Doc 8973, like how other critical security measures are managed and audited.
- **Competency Development for USAP-CMA Auditors**: Ensure that all USAP-CMA auditors are trained and certified in cyber security auditing, emphasizing knowledge of relevant standards and frameworks.

3. ACTION BY THE CONFERENCE

3.1 The Conference is invited to note the information contained in this Paper**.**

— END —