



FOURTEENTH AIR NAVIGATION CONFERENCE

Montréal, Canada, 26 August to 6 September 2024

- Agenda Item 4: Hyper-connectivity of air navigation system**
4.2: Cybersecurity and information system resilience

UNITED ARAB EMIRATES' COMMITMENT TO ENHANCING GLOBAL AVIATION CYBERSECURITY

(Presented by the United Arab Emirates)

EXECUTIVE SUMMARY

This paper details the United Arab Emirates' initiatives to enhance aviation cybersecurity. It outlines the development and ongoing refinement of cyber sSecurity measures aligned with ICAO strategies and action plan by the establishment of a National Aviation Cyber Security Committee. These measures are integral to the United Arab Emirates' Aviation Cyber Security Strategy, which adopts innovative approaches to address current and future cyber threats. Additionally, the United Arab Emirates is dedicated to international cooperation, offering to share its strategies and learnings to support other states in advancing their aviation cybersecurity frameworks. This commitment enhances the resilience of both national and international aviation landscape against cyber threats.

1. INTRODUCTION

1.1 Ensuring the security of national air navigation services against cyber threats is critical for maintaining safety and operational integrity in the aviation sector. The United Arab Emirates' strategic initiatives in developing a robust cybersecurity framework have set a precedent within the aviation industry. This paper highlights the pivotal role these efforts play in reinforcing the cyber resilience of national air navigation services.

1.2 The United Arab Emirates' approach to cybersecurity aligns with global standards and regional directives, ensuring comprehensive protection mechanisms are in place. The collaboration with international bodies and adherence to guidelines such as those outlined by the International Civil Aviation Organization (ICAO) have been instrumental in the formulation of a cohesive national aviation cybersecurity strategy.

1.3 The proactive measures and continuous improvements implemented demonstrate a commitment to integrating cybersecurity at all levels of operations. This integration is critical for adapting to the evolving cyber threat landscape and for aligning with international cybersecurity practices in civil aviation.

1.4 By adopting advanced cybersecurity protocols and fostering a culture of cyber awareness, The United Arab Emirates' strategies enhance not only national but also regional cyber resilience. These efforts contribute significantly to the overall security posture of the global aviation network, showcasing the effectiveness of national initiatives in a global context.

1.5 The paper advocates for increased collaboration and shared responsibility among ICAO Member States and industry stakeholders. Emphasizing the successful strategies employed by the United Arab Emirates, it calls for a unified approach to fortify defenses against cyber threats and to maintain the integrity and resilience of air navigation services worldwide.

2. DISCUSSION

2.1 The creation of a national aviation cyber security committee represents a strategic step toward enhancing collaboration between State-level cybersecurity authorities and aviation stakeholders. This committee facilitates ongoing dialogue, coordination and integrated cybersecurity efforts across all sectors of aviation, ensuring a unified approach to national security challenges

2.2 The formulation of a comprehensive aviation national cybersecurity strategy, alongside the specific United Arab Emirates upper airspace air navigation services Cyber Security Strategy, underscores our commitment to safeguarding digital assets against evolving cyber threats. This strategic approach is bolstered by detailed policies, procedures and action plans, ensuring alignment with the objectives and measures outlined in the Cybersecurity Action Plan to enhance resilience across the aviation sector.

2.3 The development and continuous enhancement of the regional Air Traffic Management (ATM) Data Cyber Security Portal (adcsportal.ae) signify a proactive approach to regional cybersecurity. This platform facilitates better collaboration and information sharing, as outlined in the action plan, enhancing situational awareness and fostering a proactive cybersecurity posture.

2.4 Execution of periodic State-level cybersecurity audits on operational systems ensures a rigorous assessment of existing security controls, and proactive identification and mitigation of vulnerabilities. This practice is vital for maintaining a secure operational environment, as outlined in the action plan, ensuring continuous improvement and adaptation to the cyber threat landscape.

2.5 Establishment of a Security Operation Center (SOC) enhances capabilities in monitoring, detecting and responding to cyber incidents in real-time. This initiative is pivotal for both critical and non-critical systems and services, integrating seamlessly with global efforts to strengthen cybersecurity incident management and emergency planning as emphasized in the action plan.

2.6 Ongoing enhancements to the MSB (Minimum Security Baseline) Volumes, led by United Arab Emirates initiatives, reflect our commitment to maintaining alignment with the latest industry standards and frameworks. This continual improvement process ensures that our cybersecurity measures remain robust and effective, as advocated by the action plan's emphasis on adopting and updating cybersecurity policies and strategies regularly. Furthermore, the United Arab Emirates has been instrumental in leading the development of regionally agreed MSB, setting a standard that fosters greater regional cooperation.

2.7 Enforcement of MSB compliance across all systems and vendors at United Arab Emirates upper airspace air navigation services is crucial for maintaining the confidentiality, integrity and availability of services. This rigorous compliance framework supports the action plan's directives for robust governance and accountability in managing cyber risks, promoting a standardized approach to cybersecurity across the industry.

2.8 A proposed implementation of the MSB Governance Center (MSBGC) to ensure systematic, transparent and consistent application of the MSB across all systems and vendors. This initiative mirrors the structured and strategic approach advocated in the action plan, enhancing the implementation and monitoring of cybersecurity measures across the board.

2.9 Deployment of state-of-the-art, multi-tier security infrastructure to support Secure System-wide Information Management (SWIM) Services accessible worldwide exemplifies our commitment to advanced technological integration. This aligns with the action plan's emphasis on developing capacity, training and cybersecurity culture to manage and mitigate cyber risks effectively.

2.10 The design and implementation of an in-house Public Key Infrastructure (PKI) at United Arab Emirates upper airspace air navigation services highlight our dedication to secure and trusted digital communications. This initiative is in line with the latest Trust Framework Guidelines and supports the action plan's call for robust information and communication technology security.

2.11 Regular cyber security training, workshops, and awareness sessions for all staff underscore the importance of human factors in cybersecurity. This initiative complements the action plan's focus on capacity building, training and fostering a cybersecurity culture to mitigate risks associated with human error.

2.12 Introducing basic cybersecurity skills as part of the communications, navigation, and surveillance (CNS) air traffic safety electronics personnel (ATSEP) certification equips our technicians and engineers with essential knowledge and tools. This proactive educational approach aligns with the action plan's strategy to enhance the cybersecurity qualifications of personnel involved in critical aviation roles.

3. **CONCLUSION**

3.1 The Conference is invited to take note of:

- a) the comprehensive initiatives implemented by the United Arab Emirates in enhancing aviation cyber security, which reflect a robust commitment to safeguarding its digital airspace infrastructure;
- b) the strategic frameworks established under the United Arab Emirates' Aviation Cyber Security Strategies, which incorporate innovative approaches to proactively address and adapt to emerging cyber threats and future challenges; and
- c) the United Arab Emirates' willingness to collaborate with other States in order to support and strengthen the global aviation cyber security landscape.

— END —