International Civil Aviation Organization

WORKING PAPER

AN-Conf/14-WP/202
31/7/24
(Information Paper)
English only

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

CYBER RESILIENCY IN THE NATIONAL AIRSPACE SYSTEM

(Presented by the United States)

EXECUTIVE SUMMARY

The United States National Airspace System is a network of both controlled and uncontrolled airspace, both domestic and oceanic that provides daily air traffic services to more than 45 000 flights and 2.9 million airline passengers traveling across its more than 29 million square miles of area. Since the Federal Aviation Administration (FAA) was formed as a federal agency in 1958, the national airspace system has increasingly strengthened its operational resiliency to withstand natural and man-made events to keep United States' skies ever safer for the flying public. The FAA is also working to strengthen the cyber resiliency of the national airspace system by working to deliver enterprise-wide improvements, and illustrate what measures are being taken to evaluate and validate the efficacy of these measures, including the training of its workforce to ensure the national airspace system can withstand a cyberattack today and in the future.

1. INTRODUCTION

1.1 The airspace above the Unites States, its territories and the Freely Associated States in the Pacific, is controlled by a network of facilities, systems, services, personnel, and procedures that collectively comprise the national airspace system. The area of the national airspace system that is controlled by the Federal Aviation Administration (FAA) extends from airport ground level through departure/approach to enroute elevations as high as 60 000 feet and covers more than 29 million square miles.

1.2 The FAA operates nearly 200 national airspace systems and services involving more than 74 000 pieces of aviation safety equipment and services located across the United States, its territories, and the Freely Associated States to ensure passengers and cargo move through its controlled airspace with the highest levels of safety, reliability and efficiency.

1.3 The evolution of the "Internet of Things", 5G technologies, quantum computing and other emerging technologies have broadened our ability to connect and improve productivity. They have also fueled a growth in the threat of cyber-attacks against civil aviation targets, including its systems and its personnel that use these advancements to create increasingly sophisticated and malicious methods of unlawful interference against critical infrastructure.

1.4 To counter these increased threats, the FAA is strengthening the operational and cyber resiliency of the national airspace system. They are similar in fundamental restoration and recovery objectives, but their purposes are distinctly different.

1.4.1 Operational resilience is an organization's ability to respond to and overcome adverse circumstances during operation that might cause financial loss or disrupt business services. For the FAA, this means its ability to minimize disruption to the flying public and respond and recover air navigation services in a timely manner should an impact occur.

1.4.2 National Institute of Standards Technology (NIST) Special Publication (SP) 800-160, Volume 2 defines cyber resiliency as "The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." Information technology (IT) systems, operational technology systems, and other infrastructure are dependent on cyber resources. These resources are the technological elements that enable the system to function. Cyber resiliency factors incorporate the actions of people and the evolving threat landscape.

1.4.3 This paper will focus on measures and activities the FAA is undertaking to improve the cybersecurity resiliency of the national airspace system, offering insights that will serve to benefit ICAO member states for the collective strengthening of global cyber resilience for the aviation ecosystem.

2. DISCUSSION

2.1 The FAA operates the national airspace system and is working to increasingly strengthen the cyber resiliency of the national airspace system through an integrated instantiation of strategic objectives that are moving defenses from legacy static, network-based perimeters to one that holistically focuses on authenticating, segmenting, and monitoring users, assets, and resources within the network.

2.2 A major component of the FAA's strategy to improve cyber resiliency in the national airspace system involves building segmented operating environments to protect mission critical and mission essential systems and services. Segmentation is established with enterprise cybersecurity capabilities that are configured with tailored protections for each operating environment based on the criticality of assigned systems and services. Boundary protections conforming to agency zero trust objectives provide control and accountability for access control and data transfer between operating environments, other FAA administrative environments, and to the FAA's domestic and international partners.

2.3 In addition to the segmentation of systems and services, the FAA has implemented an enterprise-wide cybersecurity enhancement program to reinforce the cyber resiliency of the national airspace system. The overall objective of this program is to deliver an integrated portfolio of enterprise common services solutions that balance operational enhancements with cybersecurity risk while considering system availability, cost and schedule to improve overall safety and efficiency. These enterprise common services solutions are foundational protections seen as prerequisites for further FAA modernizations currently in development (e.g., cloud integration, time-division multiplexing to Internet Protocol (TDM-IP) conversion, automation evolution, etc.). Features of this program includes:

2.3.1 Managed enterprise security protections: Managed enterprise security protections provide the enterprise common services infrastructure for security capabilities to enable integration of cybersecurity workflows and posture management with standing operational processes and procedures to create a seamless, coordinated, and expedited process for threat intelligence sharing and incident recognition/response.

2.3.2 Security enterprise asset management (SEAM): Provides a centralized capability to support collection of specific detailed characteristics of FAA assets across each operating environment for performing cyber monitoring and response capability. Its features include authenticated connections to perform hardware asset management, software asset management (including malware management), configuration setting management, common vulnerability management and endpoint detection response.

2.3.3 Centralized national airspace system software security management (CSSM): Improves the cyber security posture of the national airspace system by providing a centralized capability for security patch and malicious code protection updates; establish a standard secure method to access critical security configuration updates; and reduce the risk of security compromise. This will support a more reliable and resilient operating national airspace system infrastructure within each operating environment.

2.3.4 National airspace system cyber management system improvement (NCMS): Performs an expansion and technology refresh for a legacy centralized FAA system security event capture and monitoring service. This initiative expands existing NCMS services and improves logging by implementing additional hardware and software within each operating environment and integrating FAA assets with the improved service.

2.3.5 Managed enterprise security monitoring: Uses a security orchestration and automated response application to integrate authenticated cybersecurity workflows and posture management with standing operational processes and procedures to create a seamless, coordinated, and expedited process for threat intelligence sharing and incident recognition/response. These services are implemented via an enterprise common services infrastructure that provides tools to allow cybersecurity analysts to conduct threat analysis, remediation processes, and incident response activities via automated standard workflows.

2.4 Notwithstanding the FAA's measures which further harden the cyber resiliency of the national airspace system itself, the FAA has also undertaken necessary actions to engage our partners across the aviation ecosystem whose support is needed to fulfil our objectives. The FAA's ability to successfully prepare for and defend against emerging cyber threats to our globally connected system of systems necessitates the need for mutual collaboration, trust, and approach to ensure the ecosystem is resilient end-to-end.

2.4.1 Among the FAA's major partnership campaigns includes the engagement with ICAO in both the Cybersecurity Panel (CYSECP) and Trust Framework Panel (TFP) where strong bonds of trust have been forged to allow for mutual strengthening of global cyber resiliency. Products that have been developed recently by this global engagement include cybersecurity guidance materials and the *Information Security Manual* (ISM). Future initiatives include regional summits and the conduct of cyber tabletop exercises designed to test and evaluate the resilience of infrastructure, people, and processes to counter a cyber-attack.

2.4.2 Other important international engagements undertaken by the FAA that supports cyber resiliency strengthening objectives include its long-standing partnerships with the Civil Air Navigation Services Organisation (CANSO), International Air Transport Association (IATA), and the Aviation Cyber Initiative (ACI) among others. The ACI Community of Interest is composed of representatives from government agencies, industry groups, federal research facilities, academia, standards bodies and international partners.

2.5 Cyber workforce development and cyber exercises are also essential components of the FAA approach to strengthen the cyber resiliency of the national airspace system.

2.5.1 Cyber workforce development is an ongoing program that addresses the challenges FAA faces in maintaining continuing education/training in cybersecurity disciplines. The initiative enables the

FAA to recruit, train and maintain cybersecurity personnel with the requisite managerial and technical skillset to support and protect mission requirements. The approach follows the National Initiative for Cybersecurity Education Framework which provides guidelines for the development of cybersecurity role-based requirements by clearly defining what a person needs to know in order to successfully perform positional responsibilities, providing a structured foundation for training and development to support recruitment and retention, and provides a common basis to describe the depth and breadth of cybersecurity work in IT, cybersecurity and cyber-related work roles.

2.5.2 Cyber exercises are a proactive planning tool and valuable opportunity to strengthen partnerships, learn from our collective expertise, and promote cyber preparedness. They are conducted in both tabletop and functional (using lab and mock-up systems) settings by the FAA to evaluate cyber incident preparation, mitigation, response, and recovery capabilities absent the consequences of real cyber event. Lessons learned are captured, documented, and used to improve FAA programs, systems, and processes to continually reinforce the resiliency of the national airspace system.

3. CONCLUSION

3.1 The United States encourages ICAO to consider the work that the FAA is actively engaged in to further strengthen the cyber resiliency of the national airspace system and share this work with ICAO Member States so that they may benefit by increasing the cyber resilience of regional aviation so that there is, in the future, global integration, in line with ICAO recommendations.

— END —