International Civil Aviation Organization
CAR/SAM Regional Planning and Implementation Group (GREPECAS)
Eighteenth Meeting of the CAR/SAM Regional Planning and Implementation Group (GREPECAS/18)
Punta Cana, Dominican Republic, 9 to 14 April 2018

Agenda Item 3: Air navigation activities at global, inter-regional and intra-regional level

3.2 Follow-up on the implementation of global, inter-regional and intra-regional activities

Promotion of Cyber Resilience through Global Awareness and Regional Exercises

(Presented by the United States)

SUMMARY

In accordance with ICAO Assembly Resolution A39-19, the FAA is working with partners at ICAO as well as with regional partners to identify threats and risks from possible cyber incidents on civil aviation operations and critical systems and to encourage the development of a common understanding of cyber threats, risks and cyber-incident mitigation among partners.

As such, the FAA is proposing a model of regional cyber tabletop exercises utilizing facilitated discussion of scenarios designed to be an open, thought-provoking exchange of ideas on various issues regarding a hypothetical and simulated cyber incident. This exercise can be used to enhance general awareness, validate current plans and procedures, and assess the systems and activities that lie within the framework of cyber incident response and recovery. Suggested actions are included in Paragraph 4.

References:

- Assembly Resolution A39-18: Consolidated statement of continuing ICAO policies related to aviation security
- Assembly Resolution A39-19: Addressing Cybersecurity in Civil Aviation

1. Introduction

1.1 As the flying public, aviation industry, Air Navigation Service Providers (ANSPs) and Civil Aviation Authorities (CAAs) have increased reliance on communication and net-centric operations, States must work to modernize computing and network infrastructure, linking users, systems and data to provide seamless and secure access from cyber-incidents.

1.2 Cyber-incidents can affect the global aviation community or individual systems at many levels. These incidents may jeopardize communications and information exchanges between various aviation stakeholders, affecting safety and security and damaging aviation business continuity. The ability

to share cyber-related information and the application of strong standardized methods of securing data and information exchange, enhances the aviation community's ability to protect itself and limit the impacts from cyber-incidents.

1.3 To strengthen the civil aviation security posture, the FAA is undertaking an effort to identify cybersecurity risks and develop mitigation strategies across the aviation ecosystem that may impact safety and cause disruption to the operation of the National Airspace System (NAS). This cross domain strategy enables NAS components to work together as one system to ensure safe and efficient services are provided to the flying public, airlines, the US military, general aviation, and airports.

1.4 Beyond the scope of domestic cybersecurity mitigation strategies and in accordance with ICAO Assembly Resolution A39-19, the FAA is working with partners at ICAO as well as with regional partners to identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems and encourage the development of a common understanding among partners of cyber threats, risks and cyber-incident mitigation.

1.5 The FAA is proposing a model of regional cyber tabletop exercises utilizing facilitated discussion of scenarios designed to be an open, thought-provoking exchange of ideas on various issues regarding a hypothetical, simulated cyber incident, which can be used to enhance general awareness, validate current plans and procedures, and assess the systems and activities that lie within the framework of cyber incident response and recovery.

Discussion

1.6 The 39th ICAO Assembly through Resolution A39-19: Addressing Cybersecurity called upon states to inter alia:

- Identify the threats and risks from possible cyber incidents on civil aviation operations and critical systems, and the serious consequences that can arise from such incidents;
- Encourage the development of a common understanding among Member States of cyber threats and risks, and of common criteria to determine the criticality of the assets and systems that need to be protected;
- Encourage government/industry coordination with regard to aviation cybersecurity strategies, policies, and plans, as well as sharing of information to help identify critical vulnerabilities that need to be addressed;
- Develop and participate in government/industry partnerships and mechanisms, nationally and internationally, for the systematic sharing of information on cyber threats, incidents, trends and mitigation efforts;
- Establish policies and allocate resources when needed to ensure that, for critical aviation systems: system architectures are secure by design; systems are resilient; methods for data transfer are secured, ensuring integrity and confidentiality of data; system monitoring, and incident detection and reporting, methods are implemented; and forensic analysis of cyber incidents is carried out.

1.7 While work progresses at ICAO through the INNOVA Working Group to establish common and mutually agreed upon methods to protect the aviation community from cybersecurity risks through a federated framework of regulatory requirements, individual States have expressed concern in establishing and implementing cybersecurity programs.

1.8 To address these concerns and given the significant amount of communication and data information shared between the FAA and civil aviation authorities and air navigation services providers in the Caribbean, the FAA is planning to host a cybersecurity tabletop exercise, in support of developing regional best practices in response to aviation cybersecurity threats. This exercise may serve as a model for other regional cyber tabletop exercises in the future.

1.9 The planned cybersecurity tabletop exercise will be a facilitated discussion of scenarios in a formal stress-free environment. It will be an open, thought-provoking exchange of ideas on various issues regarding a hypothetical, simulated cyber incident, and can be used to enhance general awareness, validate current plans and procedures, and assess the systems and activities that lie within the framework of cyber incident response and recovery in the Caribbean region. The exercise will also focus on policies, plans, personnel contingencies, information sharing, and governmental coordination, and identify any gaps, or unclear or overlapping responsibilities.

1.10 The proposed cybersecurity tabletop exercise will bring together the FAA and Caribbean states to ensure that independent and shared information systems and networks successfully operate with cyber resiliency.

1.11 The cyber tabletop is initially planned to be a high-level discussion focused on policy and practices. Objectives for this exercise are:

- Develop and promote common understanding of cyber threats, vulnerabilities, and resultant risk across the Aviation Ecosystem
- Identify gaps in state policies and operations
- Identify and promote regional partnerships and mechanisms for information sharing on emerging threats and incident response

3.0 Conclusion

3.1 While work at ICAO on a federated framework of regulatory requirements to strengthen cybersecurity continues, more needs to be done at the State and Regional levels. By working together in regional partnership utilizing a successful model to develop a common understanding, identify gaps in policies and regulations, States can begin to develop a baseline framework to bolster cybersecurity and mitigate cyber-incidents.

4.0 Suggested Actions

4.1 The meeting is invited to:

a) Note the contents of this paper; and

b) Endorse the concept of regional cyber tabletop exercises, conducted in cooperation with ICAO Regional Offices and Member States, as outlined in Paragraph 2.6 and utilizing facilitated discussion of scenarios designed to be an open, thought-provoking exchange of ideas on various issues regarding a hypothetical, simulated cyber incident. The exercise can be used to enhance general awareness, validate current plans and procedures, and assess the systems and activities that lie within the framework of cyber incident response and recovery.

- END -