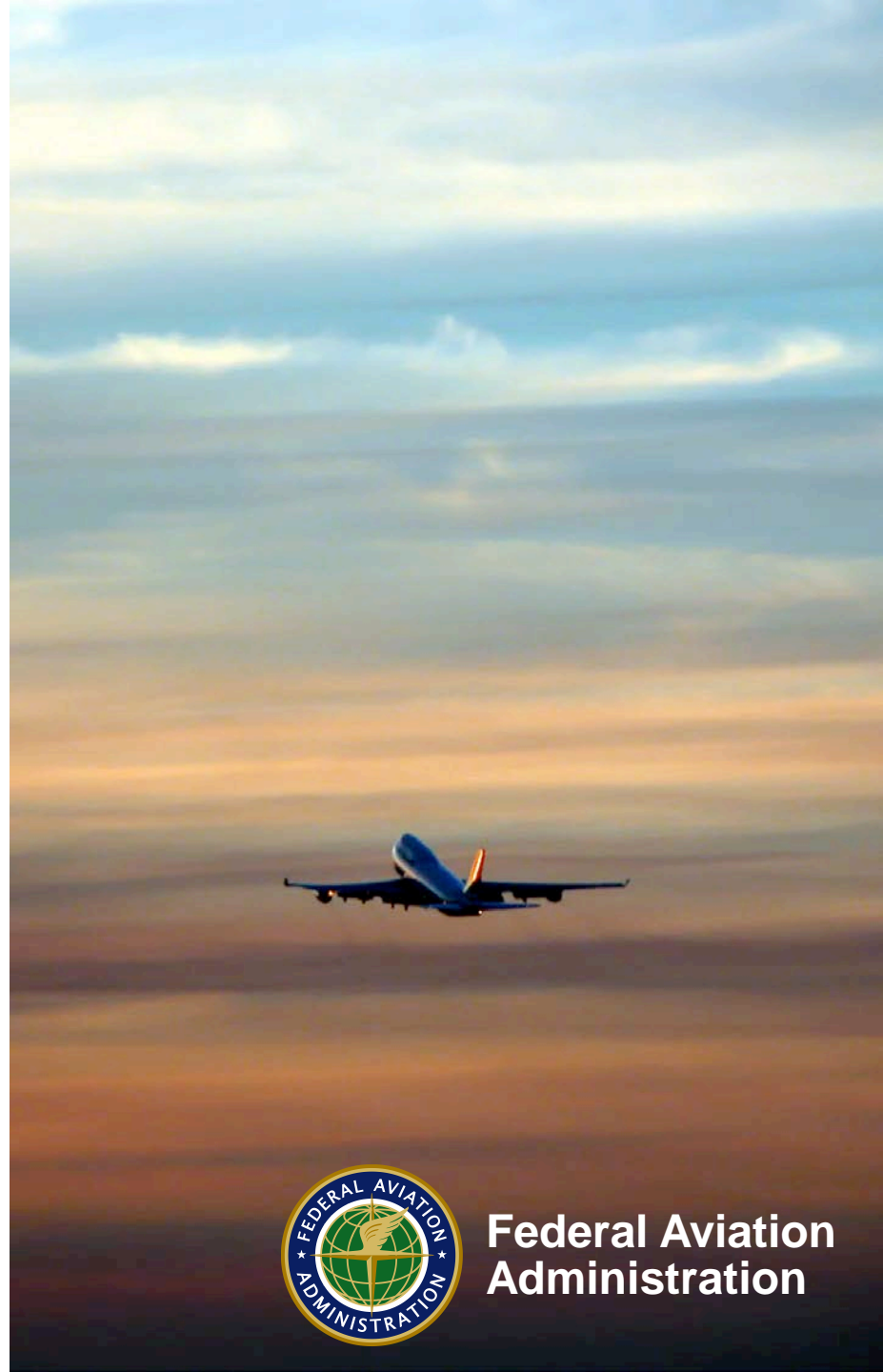# 2018 FAA Caribbean Cybersecurity Tabletop Exercise

Presented to: ICAO Cybersecurity in Aviation Workshop

By: Andrea S Freeburg, FAA Office of International Affairs

Date: Wednesday, December 5 2018

Federal Aviation Administration

Outline

- **Background**
- **Planning Timeline**
- **Objectives of the Exercise**
- **Highlights from the Event**
- **After Action Report and Template Material**
- **Lessons Learned**
- **Next Steps**

Background

- **Sep-Oct 2016:** ICAO Assembly Resolution A39-19
- **2016-2018:** FAA has internal and external discussions about developing a cybersecurity TTX
- November 2017: FAA began planning the Caribbean Cybersecurity TTX
- **July, 2018:** FAA hosted a cybersecurity TTX in support of developing regional best practices to aviation cybersecurity threats in the Caribbean
- **October, 2018:** FAA presented a working paper, which proposed a model of regional cybersecurity tabletop exercises utilizing facilitated discussions of scenarios at the ANC-13 meeting

Planning Timeline

- **Kickoff:** November, 2017
- **Identify & Invite Participants:** February, 2018
- **Develop Scenarios:** November 2017 - February 2018
- **Complete Travel & Security Logistics for Participants:** May, 2018
- **Participant Pre-meeting:** June, 2018

Highlights from the Event

Exercise: July 17-19, 2018

- July 17 – Exercise Day: Two Scenarios

- July 18 - Site Visit: FAA Command Center, Department of Homeland Security National Cybersecurity & Communications Integration Center

- July 19 - Close Out and After Action Report Discussion

Participants From:

- Barbados
- Dominican Republic
- Eastern Caribbean Civil Aviation Authority
- Guyana
- Jamaica
- Suriname
- Trinidad and Tobago
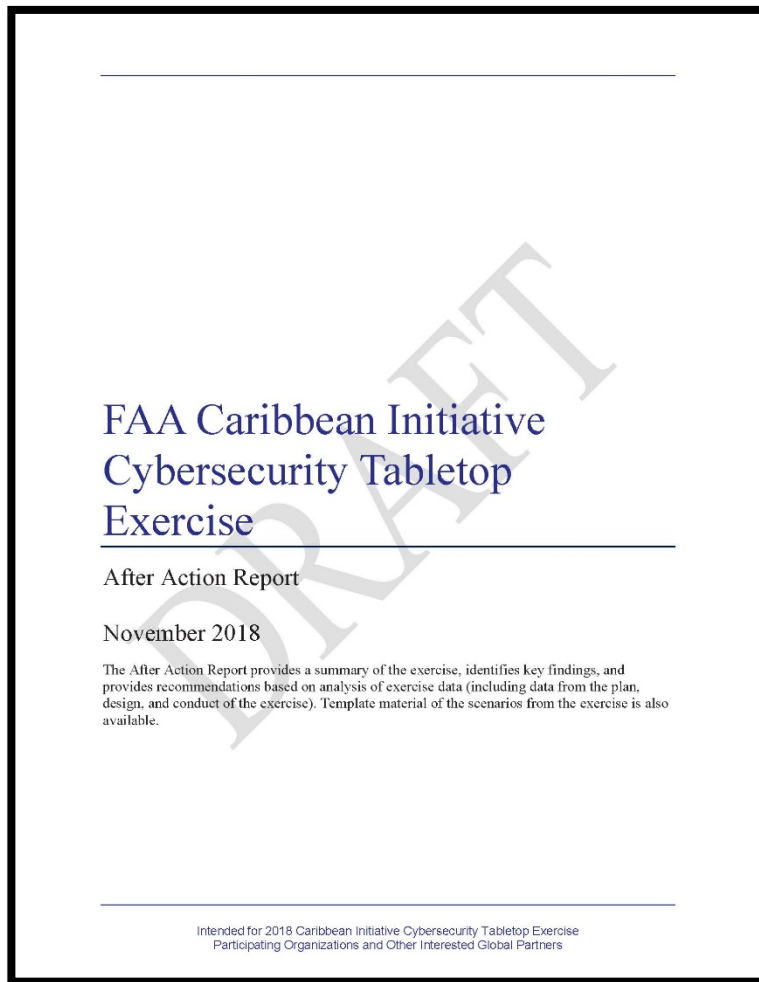- ICAO Headquarters, NACC, and SAM

Federal Aviation Administration

Objectives of the Exercise

1. Develop common understanding of cyber threats, vulnerabilities, and resultant risk across the Aviation Ecosystem

2. Identify gaps in state policies and operations

3. Identify and promote regional partnerships and mechanisms for information sharing on emerging threats and incident response

After Action Report and Template Material

FAA Caribbean Initiative Cybersecurity Tabletop Exercise

After Action Report

November 2018

The After Action Report provides a summary of the exercise, identifies key findings, and provides recommendations based on analysis of exercise data (including data from the plan, design, and conduct of the exercise). Template material of the scenarios from the exercise is also available.

Intended for 2018 Caribbean Initiative Cybersecurity Tabletop Exercise
Participating Organizations and Other Interested Global Partners

- **Drafted by FAA following the exercise and reviewed by participants**

- **Status: In the process of being finalized**

- **Once final, it will be distributed to participants and other interested individuals**

Template Material Continued

TEMPLATE:
Caribbean
Initiative Cyber
TTX

DRAFT

TEMPLATE SLIDES: This is a notional presenta...
the July 2018 FAA Caribbean Initiative Cyber...

Please contact Andrea S. Freeburg for any...
material in these slides: an...

These slides may be modified a...

Scenario 1: Day 1 AM

A: Time	B: Who delivers/receives inject (by what means)	C: Description	D: Inject Content
			E: Expected Action
0800L	ANSP 1 receives a call from Airline 1 that valid flight plan acknowledgments are not being received and the airline must submit flight plans numerous times before receiving acknowledgements from all ANSPs on route.		(1) Airline 1 Ops adds that it's not aware of any IT problems. (2) This not the first time Airline 1 has had this issue
0815L	ANSP 1 receives a follow-up call from Airline 1 that this seems to be getting worse, and is requesting ANSP 1 check its systems and circuits.		
0900L	The Regional Communications Service owner responds back to ANSP 1 reporting that the Regional Communications Service contractor confirmed the network is operational and functioning normally.		(1) Airline 1 does not respond with any additional details about the unplanned IT maintenance.
1000L	ANSP 1 receives notification from Airline 1 that they just found out they've been undergoing unplanned IT maintenance on the system that connects to ANSP 1, possibly causing its flight plan issues and intermittent data transfer.		

▶ Identify roles, responsibilities, & communication protocols
▶ Discuss the key incident response or planned executive level-decision making process ⬅ Facilitator Questions

Federal Aviation Administration

Lessons Learned

- **For the exercise:**
  - This was a very successful event in large part because participants were very engaged in the discussion
  - It was very important to have facilitators that could help guide the discussion without stifling good conversation

- **For planning:**
  - The planning team made early decisions on scope of the exercise and the objectives of the event; this helped focus planning
  - The event took 9 months of planning across multiple offices including regular workgroup meetings
  - It was very important to plan logistical coordination early including, invitations to participants and security clearance forms for site visits

Next Steps

- **FAA is working on follow-up activities to the 2018 Caribbean TTX with goals to:**
  - Continue discussions with participants
  - Identify opportunities for increasing cybersecurity in the region
  - Engage additional Caribbean countries and stakeholders

Thank you!

For more information, please contact:

Andrea S Freeburg

Foreign Affairs Specialist

Office of International Affairs

Phone: +1 (202) 267-3985

Email: andrea.s.freeburg@faa.gov