



# Florida Airports Education and Training Summit

## ***Aviation Security Tabletop Exercises: Planning, Cybersecurity Integration, and Real-World Scenarios***

Brian Krenzien

TSA - Deputy Federal Security Director (MCO)

Ms. Natasha Roman

CISA – Supervisory Protective Security Advisor (Region 4)

## 49 CFR §1542.307 Incident Management

*Section (a) Each airport operator must establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations.*

*Section (b) Immediately upon direct or referred receipt of a threat of any incidents described in paragraph (a) of this section, each operator must –*

- (1) Evaluate the threat in accordance with its security program;*
- (2) Initiate appropriate action as specified in the Airport Emergency Plan under 14 CFR 139.325; and*
- (3) Immediately notify TSA of acts, or suspected acts, of unlawful interference to civil aviation operations, including specific bomb threats to aircraft and airport facilities.*

*Section (c) Airport operators required to have a security program under § 1542.103 (c) but not subject to 14 CFR part 139, must develop emergency response procedures to incidents of threats identified in paragraph (a) of this section.*

*Section (d) – To ensure that all parties know their responsibilities and that all procedures are current, at least once every 12 calendar months each airport operator must review the procedures required in paragraphs (a) and (b) of this section with all persons having responsibilities for such procedures.*

# Aviation Cyber Initiative (ACI)

- The Aviation Cyber Initiative (ACI) is a US Government effort amongst three agencies (DHS-TSA, DoD, and DOT-FAA).
- ACI's mission is to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation's Aviation Ecosystem.
- ACI's Strategic Objectives:
  - Identify, assess, and analyze cyber threats, vulnerabilities, and consequences within the aviation ecosystem
  - Engage with aviation ecosystem stakeholders on activities for reducing cyber risk.
  - Seek potential improvement opportunities and risk mitigation strategies.
- ACI maintains a Community of Interest which presently consists of over 1200 participants. To join, please email: [ACI@faa.gov](mailto:ACI@faa.gov)
- ACI Highlights – CY 2024
  - GPS detect & respond Concept of Operations and best practices for airports:
    - Dallas-Fort Worth International Airport (DFW)
  - Cyber Rodeo Series:
    - Aviation Cyber Technical Exchange – 156 attendees
    - Securing the enterprise – 54 attendees
  - Airport Cybersecurity Training
    - Domestic – 19 airports, 28 attendees
    - International – 38 countries, 139 participants
  - ACI Wright Brothers Series #4 – Cyber TTX
  - ACI information workshops – over 150 attendees
  - Aviation Information Sharing and Analysis Center (A-ISAC) summit ([www.a-isac.com](http://www.a-isac.com))

# ACI - Sample Tabletop Exercises

## System focused Attacks

- Attacks against Industrial Control Systems (trams, buses, BHS, airport infrastructure)
- GPS Spoofing
- GPS Disruptions (jamming, outages)
- DDoS attacks on public facing websites
- Denial to critical information (e.g. NOTAMs)

## User focused attacks

- Ransomware
- Malware
- Spyware
- Data breaches

TOP 15 CYBERSECURITY THREATS				
1 Ransomware Attacks	2 IoT Vulnerabilities	3 Social Engineering and Phishing Attacks	4 Supply Chain Attacks	5 AI-Powered Cyber Threats
6 Advanced Persistent Threats (APTs)	7 Zero-Day Exploits	8 Cloud Security Risks	9 Mobile Malware and Vulnerabilities	10 Insider Threats
11 Artificial Intelligence (AI) Misuse	12 Data Breaches and Privacy Violations	13 Advanced Threat Hunting Techniques	14 Nation-State Cyber Attacks	15 Cryptocurrency-Related Threats



# ACI – In Action



## Airport Cybersecurity Training Trainee Guide

*For U.S. Airport IT Employees*



## Тренінг з кібербезпеки в аеропорту Гід стажиста

*Для IT-співробітників аеропортів США*



# ACI - Eastern European Cyber Training



- TSA conducted a multi-national cybersecurity training event in Warsaw Poland in September 2024. The effort provided elementary and mid-level training to address threats related to cybersecurity.
  - Effort jointly coordinated between TSA and Polish Civil Aviation Authority
  - Training developed by and presented by Idaho National Laboratory (INL)
  - Attended by representatives from 14 countries in Central/Eastern Europe and the Balkans
  - Included in-person cybersecurity vulnerability testing at Warsaw's Chopin International Airport

# ACI – Training Agenda



## Critical Infrastructure Cybersecurity Training

### Overview

The Critical Infrastructure Cybersecurity Training is a **week-long series** that includes four courses: Airport Cybersecurity Training, Introduction to Control Systems Cybersecurity (101), and Intermediate Cybersecurity for Industrial Control Systems Parts 1 and 2 (201 and 202). Special topics briefings on Operational Risk, Cybersecurity for Screening Equipment, and Workforce Development will also be offered during the final day of training.

An overview of each element of the training is provided below, as well as tips on how to prepare for the training.

**Approved participants will be assigned to one of two groups for the week-long training comprised of four courses and three specialized briefings.**

### Airport Cybersecurity Training

This course provides trainees with **basic to intermediate** concepts for performing cybersecurity assessments of wireless access applications at airports. Trainees will learn techniques for identifying Wi-Fi access points within the airport environment, analysis methods for determining wireless security gaps, and recommendations for improving defenses to defeat potential threats. **(1.1 Continuing Education Units (CEUs) – 11 Hours)**

By the end of this course, trainees will be able to:

1. Recognize wireless technology concepts.
2. Identify potential attack vectors.
3. Illustrate use of radio frequency (RF) capture tools.
4. Perform real-world data collection.
5. Analyze RF packet data.

### Introduction to Control Systems Cybersecurity (101)

This course introduces the basics of Industrial Control Systems (ICS) cybersecurity. This includes a comparative analysis of Information Technology (IT) and ICS architectures, understanding risk in terms of consequence, security vulnerabilities within ICS environments, and effective cyber risk mitigation strategies for the control system domain. **(0.4 CEUs – 3.5 Hours)**

### Intermediate Cybersecurity for Industrial Control Systems (201) Part 1

Building 101 course concepts, this course provides trainees with technical instruction on the protection of ICS using offensive and defensive methods. Trainees will recognize how cyber-attacks are launched, why they work, and mitigation strategies to increase the cybersecurity posture of their control system networks. **(0.7 CEUs – 7 Hours)**

### Intermediate Cybersecurity for Industrial Control Systems (202) Part 2

This course provides a brief review of ICS security. This includes a comparative analysis of IT and control system architectures, security vulnerabilities, and mitigation strategies unique to the control system domain. Accompanying this course is a sample process control network that demonstrates exploits used for unauthorized control of the equipment and mitigation solutions. This network is also used during the course for the hands-on exercises that will help the trainees develop control systems cybersecurity skills they can apply in their work. **(0.7 CEUs – 7 Hours)**

## Did You Know?

- The ACI is tri-chaired by DHS, DoD, and DOT.
- ACI works with owners and operators, manufacturers, and other partners domestically and internationally to strengthen the safety, security, and resilience of the Aviation Ecosystem.
- Improving cybersecurity at U.S. airports is a key element of this initiative.

## EVENT DETAILS

<b>DATE</b>	September 9 - 13, 2024
<b>TIME</b>	8:00 AM – 5:00 PM
<b>LOCATION</b>	Warsaw, Poland

### REGISTRATION

Please register for the training events by following the below link:

**REGISTER NOW**

## Special Topics Briefings

- **Addressing Consequence within Operational Risk** The endeavor of tackling operational risk focused on consequences is challenging even for the most resourced entity but can be advanced through a simplified approach: identifying, binning, and prioritizing the infrastructure environment. Attaining a common understanding of the infrastructure landscape as part of addressing consequences within operational risk is not easy to do or resource light, but the process outlined provides the framework to further any entity's efforts in this space.
- **Cybersecurity for Transportation Screening Equipment (TSE)**: This brief provides a high-level understanding of the real-world cybersecurity challenges TSA faces within the TSE environment. The information is a mixture of both technical and operational to allow for non-technical stakeholders to understand the risks being introduced to the environment. The presentation will discuss how TSA evaluates the TSEs, goals for the future of the technology and vision on how to secure Operational Technology within TSA.
- **Cyber-CHAMP (Competency Health and Maturity Progression) Workforce Development Framework**: By applying the framework, entities can analyze the task and responsibility composition of their current technical and management roles to inform workforce development, recruitment, structure, and alignment with security strategy.

## Who Should Take This Training?

This course is designed for **airport network and security administrators**. The following basic skills will be helpful, but are not required to participate:

- Experience in Wi-Fi configurations and basic operations
- Experience in configuring Wi-Fi access points and clients
- Basic understanding of network traffic analysis
- Working knowledge of Linux

## How Can I Prepare for This Training?

**Each participant will need to supply a laptop with a minimum of 8GB RAM, 2 USB ports and 40GB of free disk space.**

The equipment listed below will be provided to participants during the hands-on portion of the training. As this equipment will be returned upon course completion, trainees wishing to purchase similar equipment for use after the course can do so for less than \$200.00 from online retailers. Course facilitators will assist participants in setting up the purchased equipment. **The training team will have a limited number of loaner laptops for participants with technical issues.**

### Equipment (provided as needed)

- Dual-band 2.4 & 5 GHz Wi-Fi USB adapter with RT3572 or RT5572 Chipset, e.g., Alfa AWUS051NH, Panda Wireless PAU09
- Multi-port USB adapter, e.g., Pluggable USB 3.0 3-port Hub
- Texas Instrument CC2531 USB Evaluation Module Kit, 2.4 GHz

### Software (provided)

A VMWare virtual machine (VM) will be supplied to the trainees with appropriate software tools installed and configured with the above hardware so that students may run the environment in their installed VMWare Player or Workstation. Currently, MS Windows and Ubuntu flavors of Linux are supported for the VM, while Mac OSX is not supported in the class.

# Cybersecurity & Infrastructure Security Agency (CISA)

## About CISA

- CISA works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.
- As the National Coordinator for Critical Infrastructure Security and Resilience, CISA works with partners at every level to identify and manage risk to the cyber and physical infrastructure that Americans rely on every hour of every day.
- CISA works with partners to defend against today's threats and collaborate to build a more secure and resilient infrastructure for the future.
  
- **Mission:** We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
- **Vision:** A secure and resilient critical infrastructure for the American people.



# CISA Tabletop Exercises

<https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages>

## CISA Tabletop Exercises Packages (CTEP)

- Comprehensive set of resources designed to assist stakeholders in conducting their own exercises.
- Partners can use CTEPs to initiate discussions within their organizations about their ability to address a variety of threat scenarios.
- Each package is customizable and includes template exercise objectives, scenarios, and discussion questions as well as a collection of references and resources.
- Available scenarios cover a broad array of physical security and cybersecurity topics, such as natural disasters, pandemics, civil disturbances, industrial control systems, election security, ransomware, vehicle ramming, insider threats, active assailants, and unmanned aerial systems.
- CTEPs also provide scenario and module questions to discuss pre-incident information and intelligence sharing, incident response, and post-incident recovery.
- **With over 80 CTEPs available, stakeholders can find resources to meet their specific exercise needs.**

## Types of CTEP Exercises Available

- **Cybersecurity Scenarios**
  - Over 20 Cybersecurity-based threat vector scenarios including ransomware, insider threats, phishing, and Industrial Control System compromise.
- **Physical Security Scenarios**
  - Over 60 physical security Situation Manuals (SITMAN) from CISA Tabletop Exercise Packages cover topics such as active shooters, vehicle ramming, improvised explosive devices (IEDs), unmanned aerial systems (UASs).
    - Small Unmanned UAS/IED Airport Tabletop Exercise
    - Small Unmanned UAS - Nefarious Intent
    - UAS - Stadium Crash Attack
- **Cyber-Physical Convergence Scenarios**
  - Physical impacts resulting from a cyber threat vector, or cyber impacts resulting from a physical threat vector.
- **CTEP Documents**
  - Leverage pre-built templates to develop a full understanding of roles and responsibilities for exercise planners, facilitators, evaluators, and participants.
  - Templates for the initial invitation to participants, a slide deck to use for both planning meetings and conduct, a feedback form to distribute to participants post-exercise, and an After-Action Report.

# CISA Points of Contact

## Tabletop Exercise Contact:

- For more information or to request an exercise, please contact:
- [cisa.exercises@mail.cisa.dhs.gov](mailto:cisa.exercises@mail.cisa.dhs.gov)

Ms. Natasha Roman:

CISA Supervisory Protective Security Advisor

202-713-8678

[Natasha.roman@mail.cisa.dhs.gov](mailto:Natasha.roman@mail.cisa.dhs.gov)



***America's Cyber Defense Agency***

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE