CSAAP

Course One

Introduction to Cybersecurity and Airport Administration

Module Three

Airport Operations, Safety Certification, and Airfield Maintenance Cybersecurity

Overview of the operational, safety, security, and maintenance functions of an airport under Part 139, Part 1540, Part 1542 and their relationship to cybersecurity.

Sponsored by the US National Science Foundation

Cuyahoga Community College

Agenda

- Airport Safety & Part 139 Certification
- Airfield Maintenance & Operational Data Integrity
- Specialized Airport Safety Programs (SICP, ARFF, WHMP)
- Airport Emergency Management & Communications Security
- Airport Security: Regulations, Programs, and Systems (ASP, PACS, CCTV)

Objectives

- Evaluate integrity/availability of historical/operational data (1.3)
- Design role-based access control (1.5)
- Recall ATC cyber risks (2.1)
- Explain encryption in comms (2.2)
- Develop cyber incident response for ops systems (2.5)
- Secure governance/legal data (ASP related) (3.4)

Airport Safety & Part 139 Certification

- **Safe Airport Operation:** Shared responsibility (FAA, Sponsor, Users).
- **Title 14 CFR Part 139:** Certification of Airports serving scheduled air carrier aircraft with >9 seats (or unscheduled >30 seats).
- **Airport Operating Certificate (AOC): Issued** by FAA, signifies compliance.
- **Airport Certification Manual (ACM):** FAA-approved document detailing how airport complies with Part 139. Living document.

Airport Safety & Part 139 Certification (Cont'd)

- **Key ACM Elements:** Lines of succession, airport familiarization, self-inspection, maintenance, safety areas, ARFF, snow/ice control, wildlife, etc.
- **Cybersecurity Concerns**
  - *The ACM itself is a critical document.*
  - *If digital, its integrity and availability must be ensured.*
  - *Records of compliance (inspections, training) are important and often digitized.*

Airfield Self-Inspections

- **Part 139 Requirement:** Daily self-inspections.
- **What to Inspect:** Pavement, markings, lighting, safety areas, NAVAIDS, wildlife, construction, public protection, fuel farm, ARFF.
- **Record Keeping:** At least 12 CALENDAR months (for regular inspections).
- **NOTAM System (Notice to Air Missions):** Disseminates info on unsafe conditions. Airport responsibility to issue.

Airfield Self-Inspections (Cont'd)

- **Cybersecurity Concerns:**
  - *Integrity of digital inspection logs is crucial for compliance and safety analysis.*
  - *Availability of these logs for audits.*
  - *Integrity and availability of the NOTAM system (and data feeds to it) are critical for flight safety. Unauthorized or erroneous NOTAMs could be dangerous.*

Airfield Maintenance Standards

- **Pavement Management Programs (PMP):** Systematic approach to maintaining pavements (cracking, FOD, rubber buildup).
- **Markings & Signs:** Must be conspicuous, conform to standards.
- **Airfield Lighting:** Runway/taxiway edge lights, threshold lights, approach lights, PAPIs, REILs. Control systems.
- **Cybersecurity Concerns:**
  - *PMP software/databases: Integrity of data for decision-making.*
  - *Digital records of marking/signage maintenance.*
  - *Airfield lighting control systems (often OT/SCADA): Vulnerable to unauthorized control leading to safety issues (e.g., turning off runway lights, incorrect PAPI indication). Availability is important.*

NAVAIDS & Public Protection

- **Navigational Aids (NAVAIDS):** Owned/operated by FAA (ILS, VOR, NDB) or airport (PAPIs, REILs, some AWOS).
- **Airport responsibility:** Monitor status, protect from damage, report outages.
- **Public Protection:** Fencing, gates, access control to prevent inadvertent entry to movement areas.
- **Cybersecurity Concerns:**
  - *Integrity of data feeds from airport-owned NAVAIDS (e.g., AWOS) to pilots/ATC.*
  - *Protection of monitoring systems for FAA NAVAIDS.*
  - *Cybersecurity of systems controlling public access gates (linking to PACS).*

Key Airport Safety Programs (SICP, ARFF, WHMP)

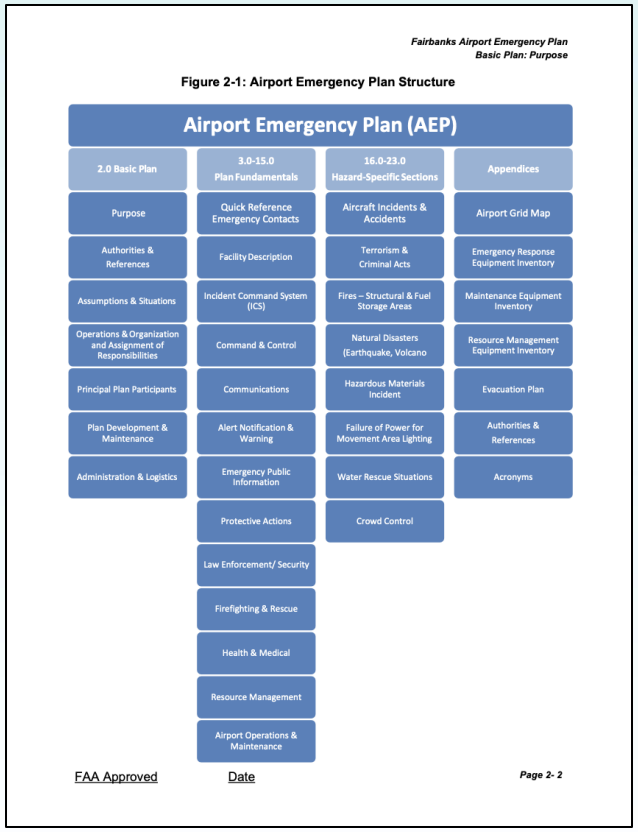
- **Snow and Ice Control Plan (SICP):** Procedures for snow removal, chemical use, airfield condition reporting.
- **Aircraft Rescue and Fire Fighting (ARFF):** Part 139 requirement. Index based on longest air carrier aircraft & frequency. Equipment, staffing, training, response times.
- **Wildlife Hazard Management Plan (WHMP):** Assesses hazards, outlines mitigation. Required if wildlife events occur.
- **Cybersecurity Concerns**
  - *Digital SICPs, airfield condition reporting systems (FICONs).*
  - *ARFF: Dispatch systems, training records, equipment maintenance logs.*
  - *WHMP: Strike databases, habitat management plans, dispersal logs.*

Airport Emergency Management (AEP, NIMS/ICS)

- **Airport Emergency Plan (AEP):** Required by Part 139. Comprehensive plan for responding to various emergencies.
- **AEP Contents:** Command & control, communications, alert procedures, mutual aid, medical, media, etc.
- **National Incident Management System (NIMS):** National standard for incident management. Provides consistent framework.
- **Incident Command System (ICS):** Standardized, on-scene management structure within NIMS. Scalable.

Airport Emergency Management (Cont'd)

- **Cybersecurity Concerns:**
  - *Securing digital AEPs (confidentiality of response plans, integrity).*
  - *Cybersecurity of Emergency Operations Center (EOC) systems, data, and displays.*
  - *Ensuring redundant/secure communication channels.*



Fairbanks Airport Emergency Plan
Basic Plan: Purpose

Figure 2-1: Airport Emergency Plan Structure

Airport Emergency Plan (AEP)

2.0 Basic Plan	3.0-15.0 Plan Fundamentals	16.0-23.0 Hazard-Specific Sections	Appendices
Purpose	Quick Reference Emergency Contacts	Aircraft Incidents & Accidents	Airport Grid Map
Authorities & References	Facility Description	Terrorism & Criminal Acts	Emergency Response Equipment Inventory
Assumptions & Situations	Incident Command System (ICS)	Fires – Structural & Fuel Storage Areas	Maintenance Equipment Inventory
Operations & Organization and Assignment of Responsibilities	Command & Control	Natural Disasters (Earthquake, Volcano	Resource Management Equipment Inventory
Principal Plan Participants	Communications	Hazardous Materials Incident	Evacuation Plan
Plan Development & Maintenance	Alert Notification & Warning	Failure of Power for Movement Area Lighting	Authorities & References
Administration & Logistics	Emergency Public Information	Water Rescue Situations	Acronyms
	Protective Actions	Crowd Control	
	Law Enforcement/ Security		
	Firefighting & Rescue		
	Health & Medical		
	Resource Management		
	Airport Operations & Maintenance		

FAA Approved Date

Page 2- 2

Airport Communications Center (ACC) & IROPS

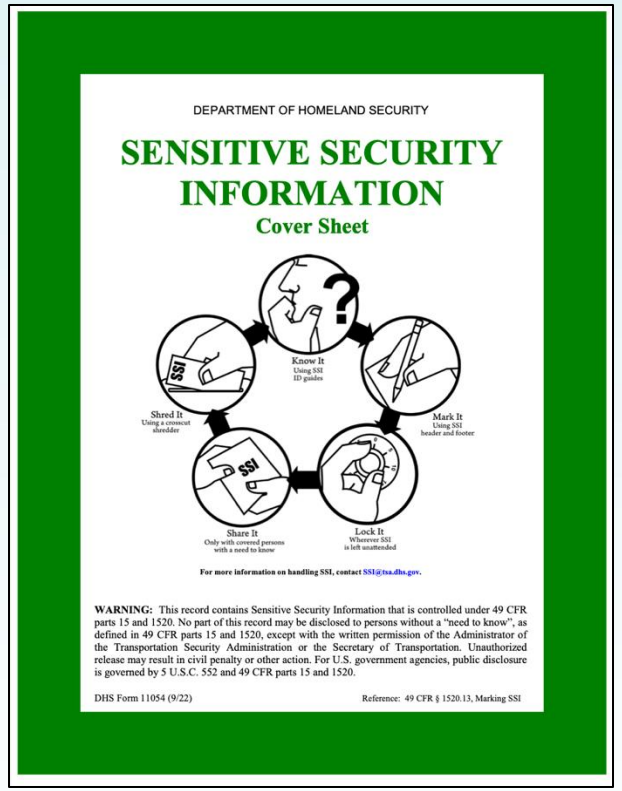
- **Airport Communications Center (ACC) / Dispatch:** Hub for airport operational comms, alarm monitoring, dispatching resources (Ops, ARFF, Police, Maintenance).
- **Irregular Operations (IROPS):** Events disrupting normal ops (weather, security, system outages). AEP often activated.
- **Cybersecurity Concerns:**
  - *ACC/Dispatch systems: Integrity and availability of Computer Aided Dispatch (CAD), phone systems, radio networks.*
  - *Protecting communication networks from jamming, eavesdropping, or disruption, especially during IROPS or emergencies.*
  - *Ensuring data flowing through ACC (incident details, resource status) is accurate.*

Airport Security Overview (ATSA, TSA Regs, ASP)

- **Post-9/11:** Aviation and Transportation Security Act (ATSA) created TSA.
- **TSA Regulations:** Part 1540 (Civil Aviation Security: General Rules), Part 1542 (Airport Security).
- **Airport Security Program (ASP):** FAA/TSA-approved document detailing how an airport complies with security regs. Specific to each airport. (CM Mod 3, pp. 89-91)
- **ASP Content:** Security areas, access control, credentialing, LEO requirements, contingency plans, training. Often SSI.

Airport Security Overview (Cont'd)

- **Cybersecurity Concerns:**
  - *ASP is a highly sensitive document.*
  - *Digital versions require strict access control and encryption.*
  - *Systems supporting ASP functions (e.g., training records, incident reports) need protection.*



DEPARTMENT OF HOMELAND SECURITY

SENSITIVE SECURITY INFORMATION

Cover Sheet

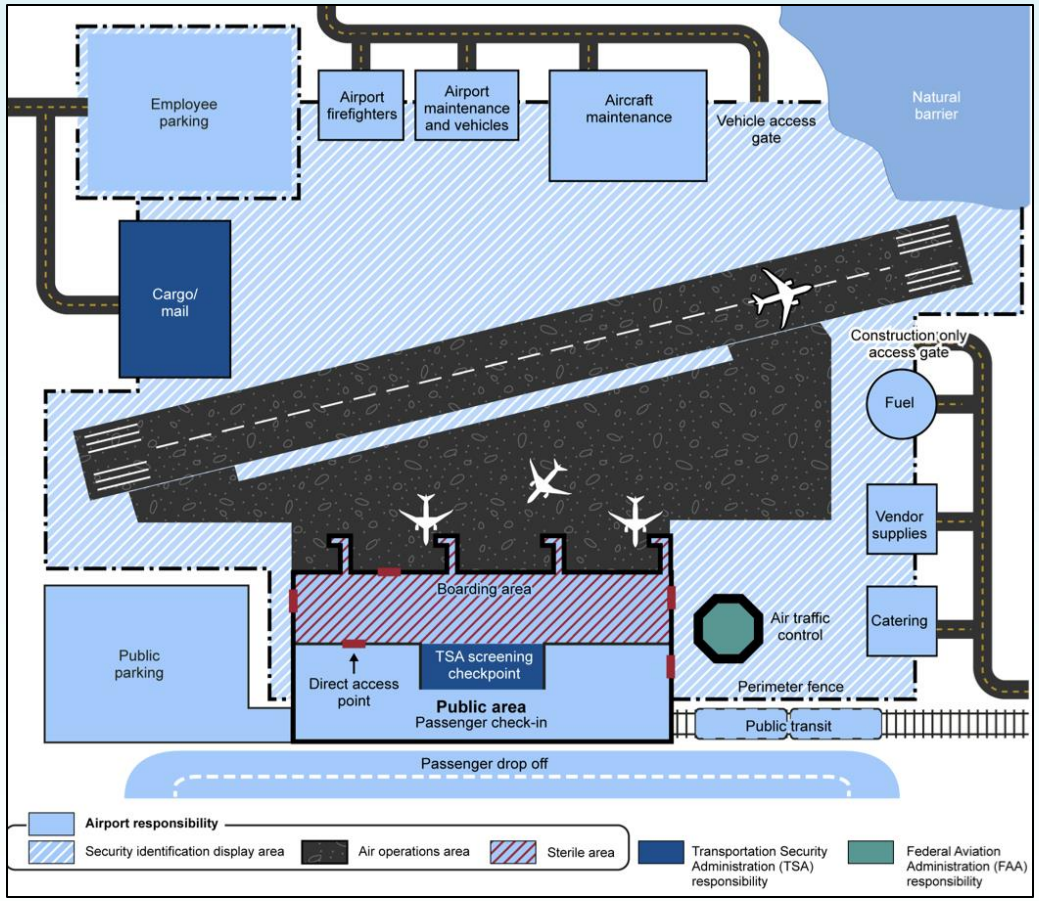
For more information on handling SSI, contact SSI@tsa.dhs.gov.

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520.

DHS Form 11054 (9/22) Reference: 49 CFR § 1520.13, Marking SSI

Airport Security Areas & Access Control

- **Security Areas:** Defined in ASP.
  - ***AOA (Air Operations Area):*** *Aircraft movement areas, ramps, safety areas.*
  - ***SIDA (Security Identification Display Area):*** *Area requiring display of airport-approved ID.*
  - ***Sterile Area:*** *Post-passenger screening, prior to boarding.*
  - ***Secured Area:*** *Highest level, includes SIDA with more stringent access control.*



Airport Security Areas & Access Control (Cont'd)

- **Access Control & Credentialing Systems (PACS):** Manage who has access to what areas, when.
  - *Badging, biometrics, PINs.*
  - *Database of personnel, access levels, training status.*
- **Cybersecurity Concerns:**
  - *PACS database is a prime target (PII, access privileges).*
  - *Integrity of access rules, availability of the system, and confidentiality of data are critical.*
  - *Compromise could enable insider threats or unauthorized physical access.*

SLE Secured/SIDA ID Media

SLE Air Operations Area ID Media

Physical Security (CCTV) & GA Security

- **CCTV Systems:** Widely used for surveillance. Increasingly IP-based.
- **GA Airport Security:** Typically, less stringent than Part 1542, but still important.
- **Cybersecurity Concerns:**
  - ***IP CCTV:*** *Vulnerable to network attacks if not secured (default passwords, unpatched firmware, network segmentation). Video could be intercepted or manipulated.*
  - *Secure storage and access control for recorded CCTV footage.*
  - *Even GA airports using digital systems for access or record-keeping need basic cyber hygiene.*

Conclusion

- **Recap:** Airport operations, safety (Part 139), maintenance, emergency management, and security are all data-intensive and system-reliant.
- Cybersecurity is important for protecting inspection records, maintenance systems (PMP, lighting controls), NAVAID data, safety program data (SICP, ARFF, WHMP), emergency plans & comms (AEP, EOC), and security systems (ASP, PACS, CCTV).

Module 4 Preview & Questions

- Airport Operations, Safety Certification (Part 139), Airfield Maintenance, and their specific cybersecurity challenges.
- Check LMS for readings, supplemental resources, discussion board, and quiz.
- Questions?