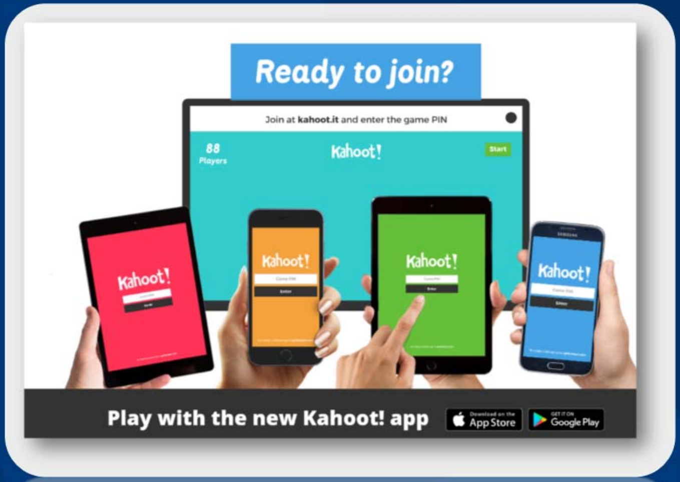
2019 AIRPORTS@ >>WORK



Please open a browser to https://www.kahoot.it or download the Kahoot! App. to participate.

Concurrent Session 1C: Cybersecurity—Federal Agencies

Grand Ballroom B

April 3, 2019 | 1:15 PM

ACI
NORTH AMERICA
AIRPORTS COUNCIL INTERNATIONAL

Panelist Agencies

Panelists

Nancy Lim (DHS CISA)
Chief of Staff for Strategy at the Office of the Assistant Secretary / Senior Cybersecurity Advisor at the Office of the Chief of Staff

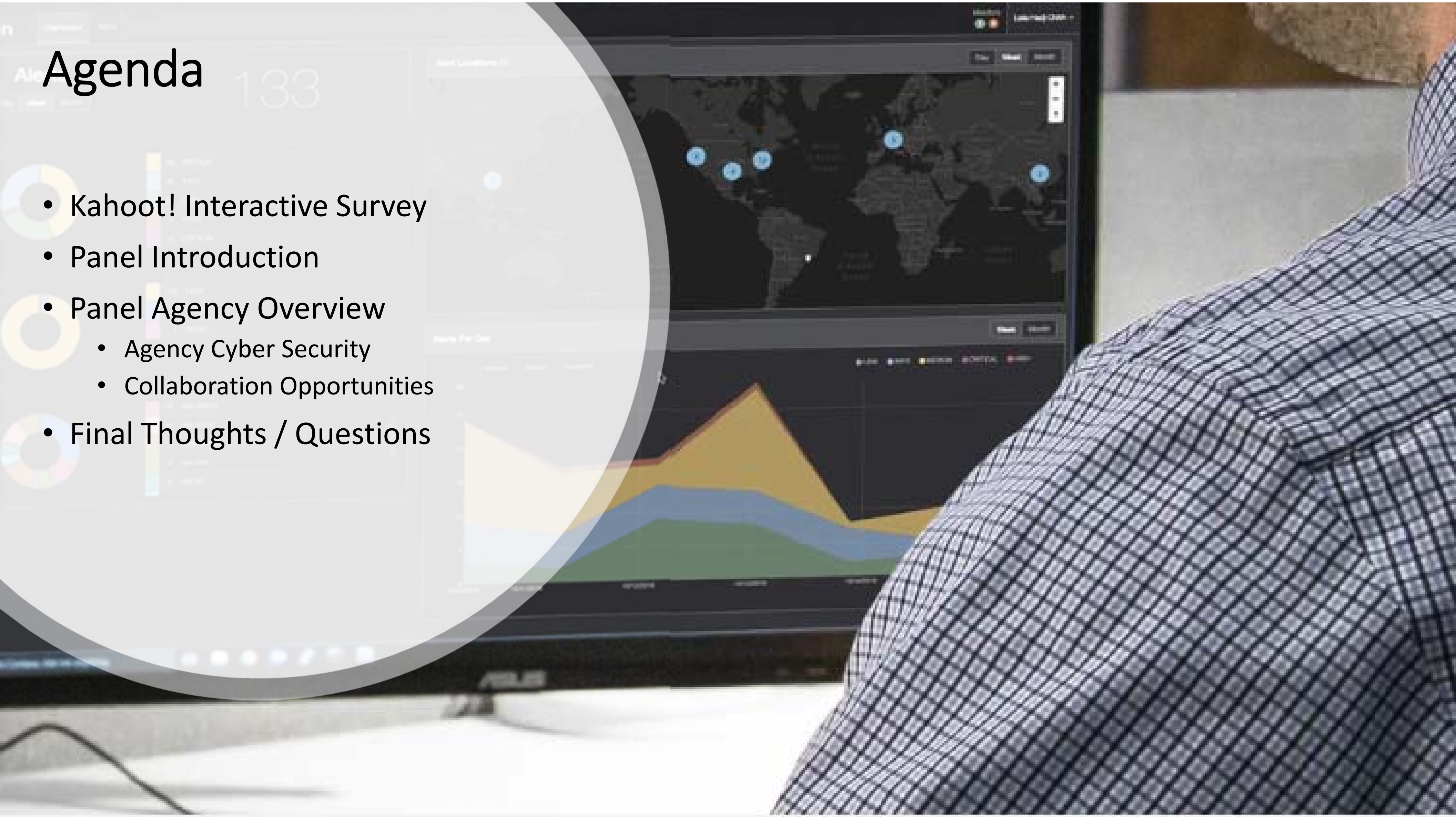
Jason Bretzinger (FBI)
Program Manager, Cyber Division, Federal Bureau of Investigation

Kelsey Erwin (FBI)
Intelligence Analyst

Isidore Venetos (FAA)
Manager, Aviation Information Security Protection R&D Federal Aviation Administration

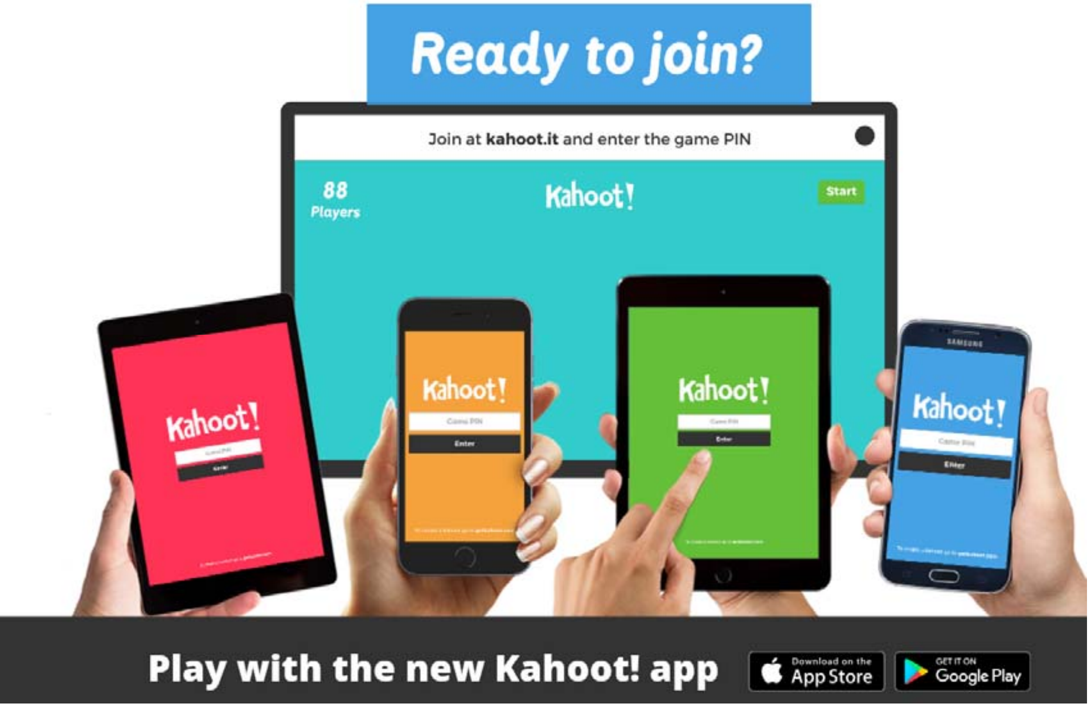
Royce Holden (DFW) (Moderator)
AVP ITS – Technology Security & Compliance (CISO)

Agenda



- Kahoot! Interactive Survey
- Panel Introduction
- Panel Agency Overview
  - Agency Cyber Security
  - Collaboration Opportunities
- Final Thoughts / Questions

Interactive Session Survey


Ready to join?
Join at kahoot.it and enter the game PIN
88 Players
Kahoot!
Start
Play with the new Kahoot! app
Download on the App Store
GET IT ON Google Play

Please open a browser to https://www.kahoot.it or download the Kahoot! App. to participate.

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

AVIATION CYBER INITIATIVE (ACI)

CISA
CYBER+INFRASTRUCTURE

Nancy Lim
April 15, 2019

ACI: Overview

- **Mission:** Reduce ***cybersecurity risks*** and improve ***cyber resilience*** to support safe, secure, and efficient operations of the Nation's Aviation Ecosystem

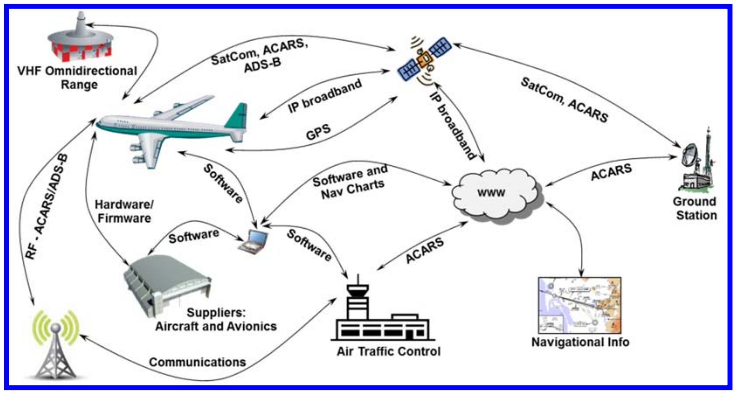
- ACI serves as an ***interagency forum*** to implement the cybersecurity objectives of the **National Strategy for Aviation Security (NSAS)**
- Tri-Chaired Task Force led by:

CISA
CYBER+INFRASTRUCTURE

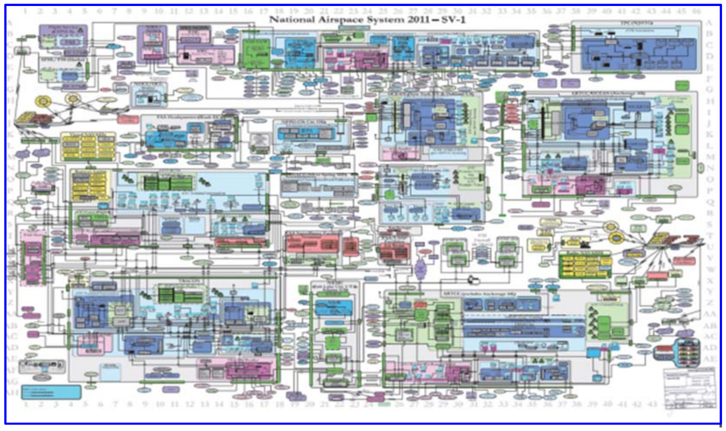
ACI: Supporting Objectives

- Facilitate U.S. Gov't efforts on cyber risk reduction of the Nation's Aviation Ecosystem with the following supporting objectives:
  - **Identify, assess and analyze cyber threats, vulnerabilities, and consequences** within the Aviation Ecosystem through research, development, testing, and evaluation initiatives,
  - Seek potential improvement opportunities and **risk mitigation strategies**,
  - Engage with Aviation Ecosystem stakeholders on activities for **reducing cyber risk**

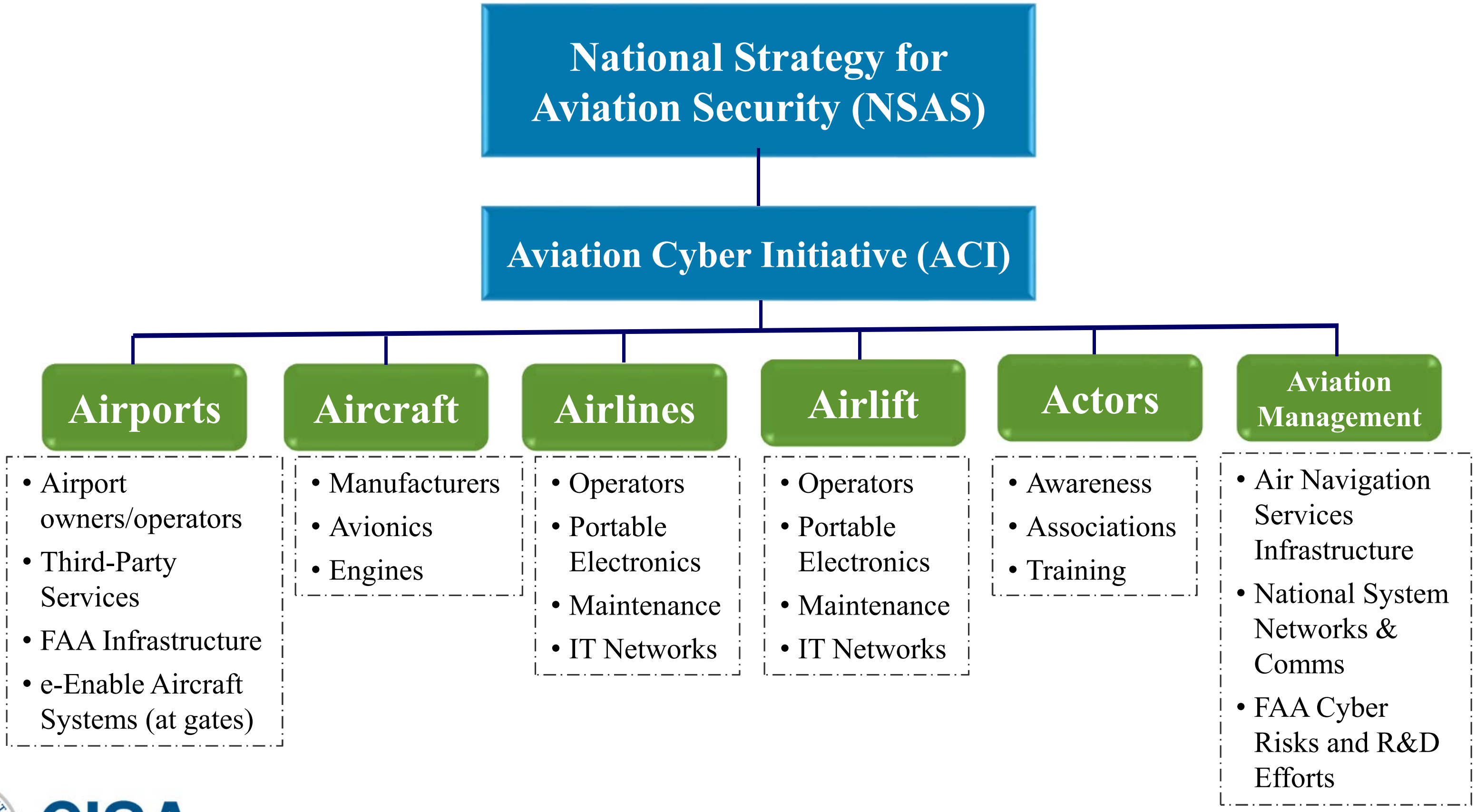
Cyber Access Pathways in Aviation Ecosystem



"Simplified National Airspace System"



ACI: The 6-As



National Strategy for Aviation Security (NSAS)

Aviation Cyber Initiative (ACI)

Airports

- Airport owners/operators
- Third-Party Services
- FAA Infrastructure
- e-Enable Aircraft Systems (at gates)

Aircraft

- Manufacturers
- Avionics
- Engines

Airlines

- Operators
- Portable Electronics
- Maintenance
- IT Networks

Airlift

- Operators
- Portable Electronics
- Maintenance
- IT Networks

Actors

- Awareness
- Associations
- Training

Aviation Management

- Air Navigation Services Infrastructure
- National System Networks & Comms
- FAA Cyber Risks and R&D Efforts

National Cybersecurity Assessments & Technical Services (NCATS) - Services

Services are provided at "no cost" to our customers

- Vulnerability Scanning (Cyber Hygiene)
- Phishing Campaign Assessments
- Reputation and Posture Monitoring
- Risk and Vulnerability Assessments
- Remote Penetration Testing
- Red Team Assessment
- Validated Architecture Design Review

Our "payment" is authorization to use anonymized, non-attributable data to enhance national situational awareness and enable our stakeholders to make data drive decisions

NCATS_INFOR@hq.dhs.gov

For more information:
cisa.gov

Questions?
Email: Nancy.Lim@hq.dhs.gov
Phone: 202-306-5964

Federal Bureau of Investigation (FBI)

FAA Cyber Research & Development

Isidore Venetos
Federal Aviation Administration
William J. Hughes Technical Center -
Aviation Research Division (ANG-E2)
Aviation Information Security Protection R&D ,
Manager
Atlantic City International Airport, NJ 08405
Isidore.venetos@faa.gov

Purpose

- **Share information about FAA cyber aviation safety risk assessment methodology**
- **Share information on security ecosystem**
- **Share Aviation Security Vision for the future**
- **Explore possible ways that SRA methodology can help Airports cyber posture**

NextGEN

NOT your typical IT networks

It is all about understanding Risk

Location: William J. Hughes Technical Center, ACY New Jersey

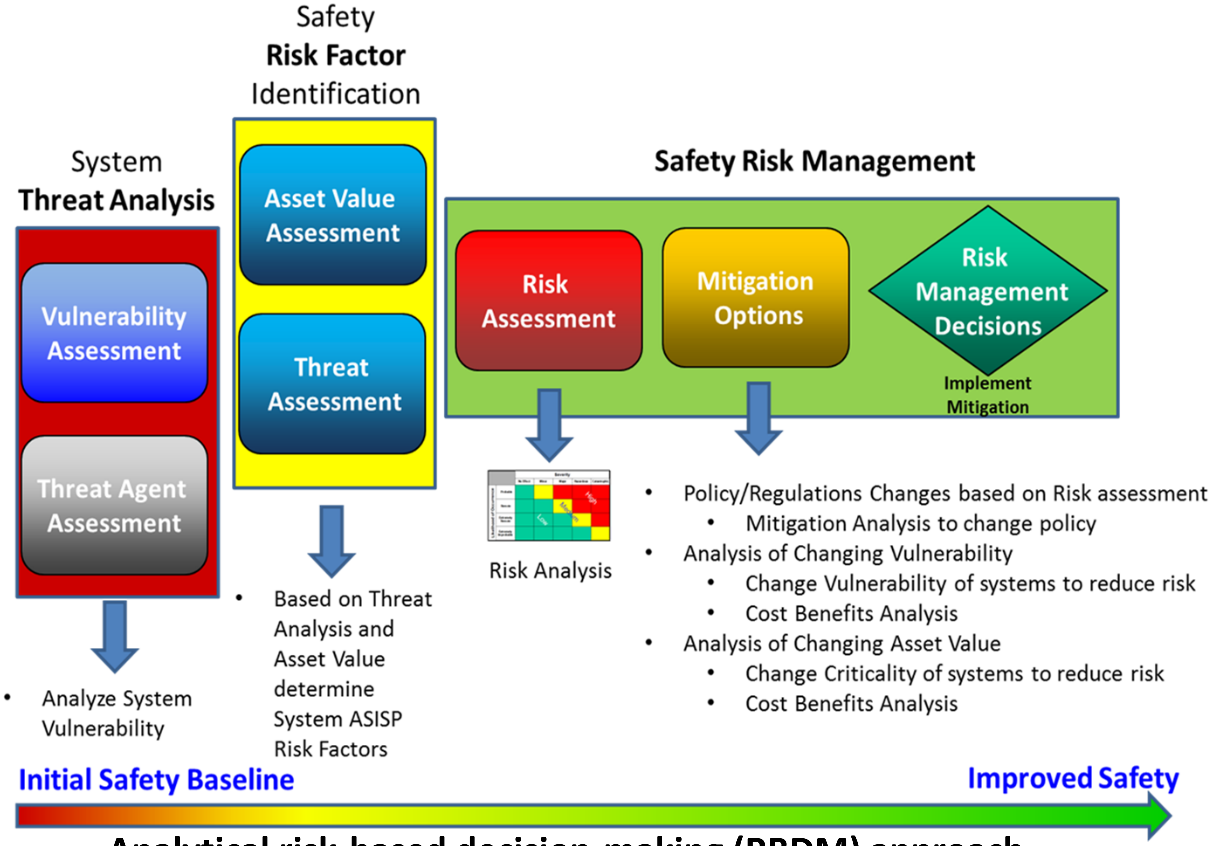
Aviation Research Division Cyber R&D Overview

- **<u>Aviation Research Division</u>** Cyber R&D Programs

  Two Broad categories of FAA Cyber research:

  - ➢ **Aviation Safety**
    - o Support development of policy, regulation, guidance
    - o *Collaborate with the aviation community*
    - o **Promote the safety culture to include information security**
  - ➢ **Innovative Cyber Capability Development**
    - o Mature innovative technologies/concepts for application into the aviation ecosystem
    - o Smart Airports of the Future testbed at ACY

Safety Risk Assessment Research Framework



- Analyze System Vulnerability

- Based on Threat Analysis and Asset Value determine System ASISP Risk Factors

- Policy/Regulations Changes based on Risk assessment
  - Mitigation Analysis to change policy
- Analysis of Changing Vulnerability
  - Change Vulnerability of systems to reduce risk
  - Cost Benefits Analysis
- Analysis of Changing Asset Value
  - Change Criticality of systems to reduce risk
  - Cost Benefits Analysis

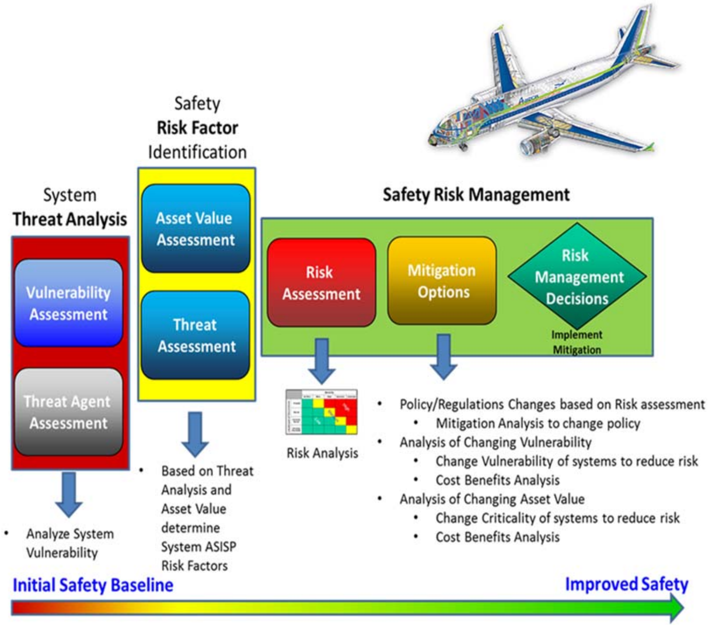
Analytical risk-based decision-making (RBDM) approach

Solutions - based approach;

Aircraft Systems Information Security Protection (ASISP)

Goal: A Risk Based Decision Making Process for assessing the risks associated with cyber attacks on aircraft

- ✓ Allows consistent standard outputs
- ✓ Structured methodology
- ✓ Repeatable and Validated processes
- ✓ Removes assessment bias
- ✓ Consistent with the Safety Management Systems (SMS)- Safety Risk Management (SRM) and Risk Based Decision Making (RBDM) principles FAA strategic initiative



- Analyze System Vulnerability

- Based on Threat Analysis and Asset Value determine System ASISP Risk Factors

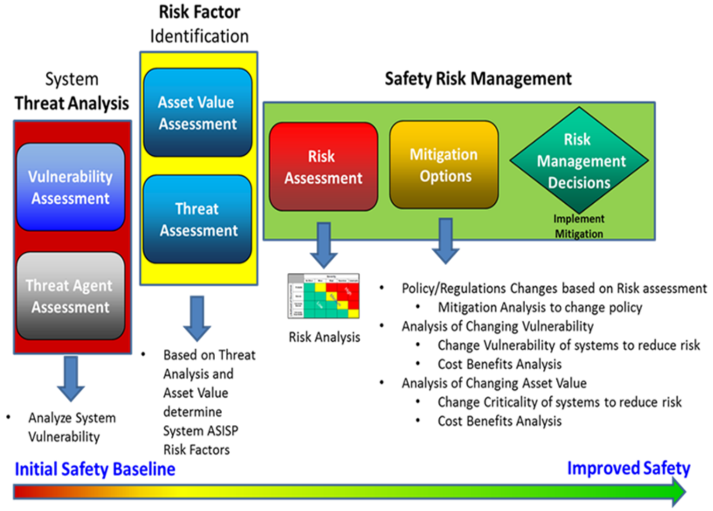
- Policy/Regulations Changes based on Risk assessment
  - Mitigation Analysis to change policy
- Analysis of Changing Vulnerability
  - Change Vulnerability of systems to reduce risk
  - Cost Benefits Analysis
- Analysis of Changing Asset Value
  - Change Criticality of systems to reduce risk
  - Cost Benefits Analysis

RBDM process can be applied to other systems beyond Aircraft to the Aviation Ecosystem

Airport Systems Information Security Protection

Goal: A Risk Based Decision Making Process for assessing the risks associated with cyber attacks on aircraft

- Allows consistent standard outputs
- Structured methodology
- Repeatable and Validated processes
- Removes assessment bias
- Consistent with the Safety Management Systems (SMS)- Safety Risk Management (SRM) and Risk Based Decision Making (RBDM) principles FAA strategic initiative



Safety Risk Factor Identification

Asset Value Assessment

Threat Assessment

- Based on Threat Analysis and Asset Value determine System ASISP Risk Factors

System Threat Analysis

Vulnerability Assessment

Threat Agent Assessment

- Analyze System Vulnerability

Safety Risk Management

Risk Assessment

Mitigation Options

Risk Management Decisions

Implement Mitigation

Risk Analysis

- Policy/Regulations Changes based on Risk assessment
  - Mitigation Analysis to change policy
- Analysis of Changing Vulnerability
  - Change Vulnerability of systems to reduce risk
  - Cost Benefits Analysis
- Analysis of Changing Asset Value
  - Change Criticality of systems to reduce risk
  - Cost Benefits Analysis

Initial Safety Baseline

Improved Safety

RBDM process can be applied to other systems beyond Aircraft to the Aviation Ecosystem such as Airports

MASSPORT & FAA
Seedling Collaboration

- **Vision: Utilize existing Aircraft Systems Information Security Protection (ASISP) cyber safety risk assessment R&D methodology to assess systems across the Aviation Ecosystem**

Initial Assessment Subject:
Automated Aircraft Docking System (SafeGate)

Program Goals

- Work with Logan Airport - MASSPORT to assess SafeGate for cyber safety issues
- Identify and assess cyber vulnerabilities and risks associated with SafeGate system implementation at Logan Airport
- Complete analytical cyber study based on *available documentation* & *cross organizational subject-matter-experts* (SME) input
- Complete a Cyber penetration testing to discover vulnerabilities
- Establish FAA seedling funding to prove the concept of applying ASISP to other complex systems beyond aircraft avionics
- Establish potential future use of FAA Airport Improvement Program (AIP) funds to conduct other cybersecurity assessments

PARTNERSHIP

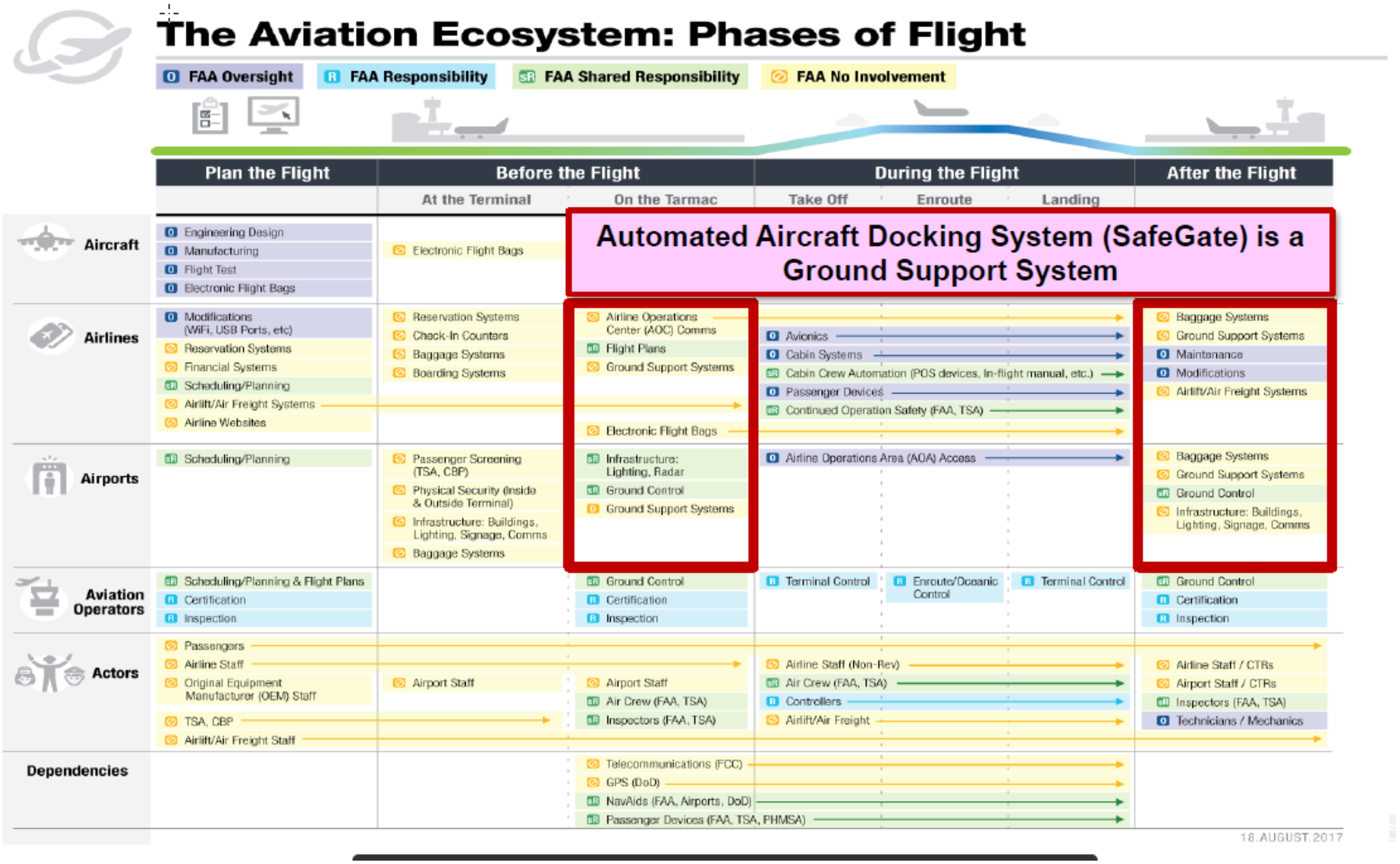
Federal Aviation Administration

MIT Lincoln Laboratory

massport

NextGEN

Aviation Ecosystem Analysis



The Aviation Ecosystem: Phases of Flight

O FAA Oversight | R FAA Responsibility | sR FAA Shared Responsibility | ⊘ FAA No Involvement

	Plan the Flight	Before the Flight		During the Flight			After the Flight
		At the Terminal	On the Tarmac	Take Off	Enroute	Landing	
Aircraft	O Engineering Design O Manufacturing O Flight Test O Electronic Flight Bags	⊘ Electronic Flight Bags					
Airlines	O Modifications (WiFi, USB Ports, etc) ⊘ Reservation Systems ⊘ Financial Systems sR Scheduling/Planning ⊘ Airlift/Air Freight Systems → ⊘ Airline Websites	⊘ Reservation Systems ⊘ Check-In Counters ⊘ Baggage Systems ⊘ Boarding Systems	⊘ Airline Operations Center (AOC) Comms → sR Flight Plans ⊘ Ground Support Systems ⊘ Electronic Flight Bags →	O Avionics → O Cabin Systems → sR Cabin Crew Automation (POS devices, In-flight manual, etc.) → O Passenger Devices → sR Continued Operation Safety (FAA, TSA) →			⊘ Baggage Systems ⊘ Ground Support Systems O Maintenance O Modifications ⊘ Airlift/Air Freight Systems
Airports	sR Scheduling/Planning	⊘ Passenger Screening (TSA, CBP) ⊘ Physical Security (Inside & Outside Terminal) ⊘ Infrastructure: Buildings, Lighting, Signage, Comms ⊘ Baggage Systems	sR Infrastructure: Lighting, Radar sR Ground Control O Ground Support Systems	O Airline Operations Area (AOA) Access →			⊘ Baggage Systems ⊘ Ground Support Systems sR Ground Control ⊘ Infrastructure: Buildings, Lighting, Signage, Comms
Aviation Operators	sR Scheduling/Planning & Flight Plans R Certification R Inspection		sR Ground Control R Certification R Inspection	R Terminal Control	R Enroute/Oceanic Control	R Terminal Control	sR Ground Control R Certification R Inspection
Actors	⊘ Passengers → ⊘ Airline Staff → ⊘ Original Equipment Manufacturer (OEM) Staff ⊘ TSA, CBP → ⊘ Airlift/Air Freight Staff →	⊘ Airport Staff	⊘ Airport Staff sR Air Crew (FAA, TSA) sR Inspectors (FAA, TSA)	⊘ Airline Staff (Non-Rev) → sR Air Crew (FAA, TSA) → R Controllers → ⊘ Airlift/Air Freight →			⊘ Airline Staff / CTRs ⊘ Airport Staff / CTRs sR Inspectors (FAA, TSA) O Technicians / Mechanics
Dependencies			⊘ Telecommunications (FCC) → ⊘ GPS (DoD) → sR NavAids (FAA, Airports, DoD) → sR Passenger Devices (FAA, TSA, PHMSA) →				

Automated Aircraft Docking System (SafeGate) is a Ground Support System

18.AUGUST.2017

The proposed cyber risk assessment Crosses multiple parts of the ecosystem

FEDERAL AVIATION ADMINISTRATION

Safety Risk Assessments

- Apply sound system engineering principles and work with the various agencies to understand the risks
- Cyber Safety Risk Assessments (SRAs) are generated for specific systems based on a repeatable methodology
- In process of establishing **Cyber Commercial Aviation Safety Team** partnering federal organizations and industry

MIT
LINCOLN
LABORATORY

APL JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

Astronautics
Corporation of America

NextGEN

Cyber Security awareness is rising

Safety & Security Culture

Trust

Aware

Learn/Train

Communicate

Proactive

Response

Work Together

- **Government has recognized importance of cyber security across aviation ecosystem**
  - **Congress, White House, FAA**
- **AVS is sponsoring ASISP R&D**
- **The FAA R&D Organization has flexibility to:**
  - **work with industry**

Safety Environment: Today

Safety

- Safety culture is very strong
  - Safety is a priority, well understood problem set of risks and solutions, proactive approach with solution sets
  - Well structured safety processes & procedures support the culture
- Outstanding historical performance record
- Commercial Aviation Safety Team (CAST)
  - Solutions based; NOT regulatory based
  - Industry coordinated solutions
- Predictable product assurance based approach
  - Likelihood is very quantitative with well documented occurrences to include outliers

Cyber Security

- Security culture is in development
  - Cyber Security is not often prioritized, not a well understood set of risks and solutions with ad-hoc approach and patch solution sets
  - Processes & Procedures being developed independently
- Sparse documented historical record
- No CAST equivalent community solution
  - Often checklist compliance based
  - Independent solution sets
- Unpredictable Cyber-based environment
  - Likelihood is not easily quantifiable since cyber security is based on vulnerabilities, actor capabilities and actor motivation

Safety Environment: Tomorrow

Safety

- Safety culture is very strong
  - Safety is a priority, well understood problem set of risks and solutions, proactive approach with solution sets
  - Well structured safety processes & procedures support the culture
- Outstanding historical performance record
- Commercial Aviation Safety Team (CAST)
  - Solutions based; NOT Regulatory based
  - Industry coordinated solutions
- Predictable product assurance based approach
  - Likelihood is very quantitative with well documented occurrences to include outliers

Cyber Security

- Security culture is strong
  - Cyber Security risks prioritized, well understood set of risks and solutions with industry wide approach
  - Well structured Processes & Procedures in place
- Historical record of threat/risks/mitigations
- CAST equivalent community solution
  - Solutions based; NOT Regulatory based
  - Consensus-based solution sets
- Managed Cyber-based environment
  - Understanding of vulnerabilities, actor capabilities and actor motivation
  - **Risk-Based Management Approach**

Industry and Government Partnership is imperative for a Strong Safety + Security Culture

Cyber Security Federal Agencies – Final Thoughts / Questions