Cyber Safety
Commercial Aviation Team
(Cyber Safety CAT)

Overview
August 20, 2019
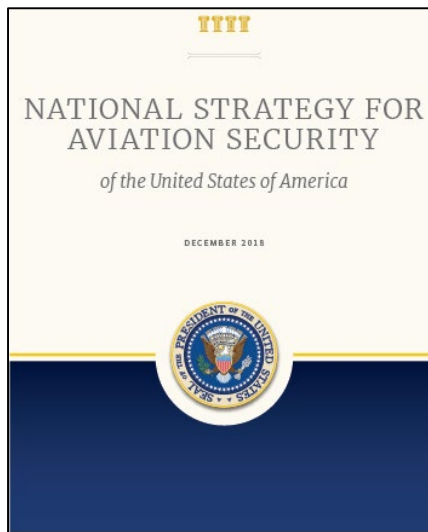
Cyber Safety For the Aviation Ecosystem

Cybersecurity awareness is rising

Safety & Security Culture

- **Aviation community has recognized importance of cybersecurity**
  - Specifically to safety across aviation ecosystem
  - White House – established strategic guidance
  - Industry – ASISP ARAC WG established recommendations
- **Need for Public and Private Partnership**
  - Collaborative partnership which establishes a trusted environment
  - Establishes formal communication channels
  - Proactive approach to raise awareness and consensus

Cyber Safety CAT Strategic Alignment

NSAS: "Desired End-State… A safe and secure aviation ecosystem. …

- **The FAA is responsible for the safety oversight of much of the Aviation Ecosystem…**
- **DHS and DOT share responsibility to coordinate infrastructure protection activities for the Transportation Sector…"**

https://www.whitehouse.gov/wp-content/uploads/2019/02/NSAS-Signed.pdf

FAA Research Activity

- **"Explore an AVS ASISP safety risk management process and integrate all of the components …with all available resources. Propose effective formal strategies, which will leverage the efforts from other government agencies and industry stakeholders. Goal to reduce the associated ASISP risks for aircraft certification, maintenance and continued operational safety."**
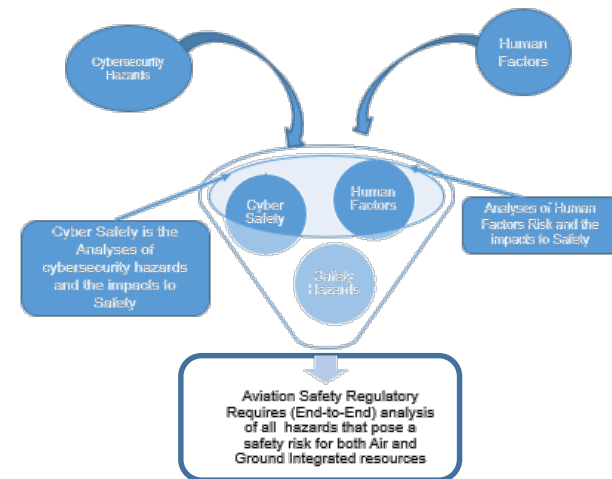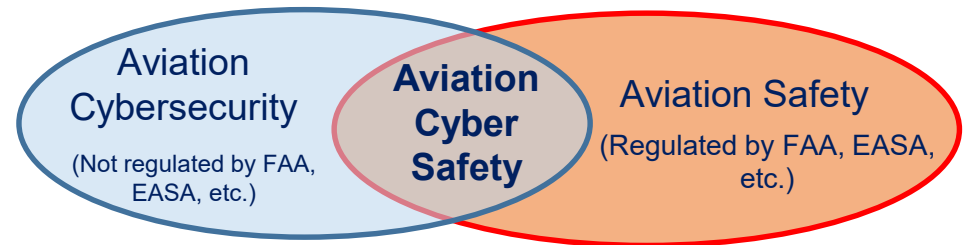
Cyber-Safety Commercial Aviation Team

Cyber Safety hazards include all threat vectors via internal and external connectivity to the **aircraft and NAS operations**, with focus on the interoperability and efficiency related safety impacts to air/ground resources that have:

- An ability to directly impact ATM services
  - Impacts to pilot decision making or aircraft control systems (Aircraft)
  - Air-to-Ground Voice and Data
- The ability to directly impact the interoperability between ATM stakeholders responsible for providing ATM critical and safety services
  - Aerodrome (airport connections to NAS/Airplane)
  - Air Navigation Service Providers (ANSP)
  - Communications providers (air, space and ground)
  - Aircraft and Avionics manufacturers
- The ability to impact airspace capacity and efficiency

International Coordinating Council of
Aerospace Industries Associations

4

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

Cybersecurity

- 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

Cybersecurity

- 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
- **Cyber Safety CAT community solution**
  - Solutions based; NOT Regulatory based
  - Consensus-based End-to-End solution sets
- **Managed Cyber-based environment**
  - Understanding of vulnerabilities, actor capabilities and actor motivation
  - **Risk-Based Management Approach**

Industry & Government Partnership is Imperative for a Strong Safety + Security Culture. AIA & FAA Aviation Research Division working together to define the approach.

Cyber Safety CAT Approach

Vision

- Key aviation stakeholders acting cooperatively to lead the US aviation community to the highest levels of commercial aviation cyber-safety by focusing on scenarios that enable proactive and continuous assessment of vulnerabilities and risks to the aviation ecosystem.

Mission

- Enable a continuous improvement framework built on the proactive identification of current and future risks, developing mitigations as needed and monitoring the effectiveness of implemented actions.
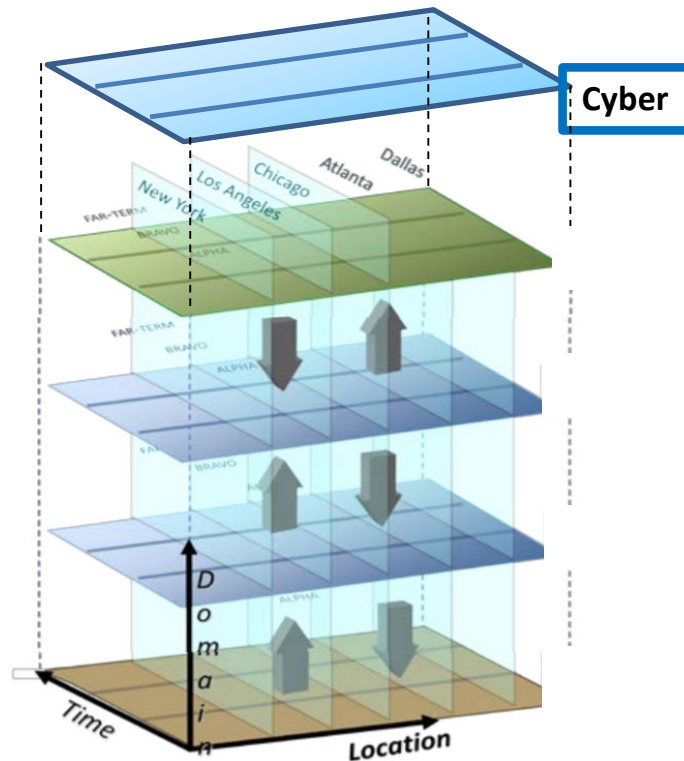
Goal

- Reduce the U.S. commercial aviation cyber-safety risk, and continue to work with our international partners to reduce cyber-safety risk world-wide across commercial aviation.

Deliverables

- Actionable mitigation recommendations for: best practices, technology development, EASA/ESCP Harmonization, ICAO Influence, Aviation Cyber Safety Incident Communications & Response Plans, guidance, policy, and if needed recommendations for regulatory consideration

Aviation Safety provides a Robust Framework to Leverage

Cyber Safety Overlay and Integration

The Complex Integration Aspects of a Capability

https://www.faa.gov/air_traffic/publications/media/ATO-SMS-Manual.pdf

➢ Cyber-Safety capabilities & controls
  - ✓ Leverage Power of Aviation Safety Community
  - ✓ Complement existing Aviation organizations, processes and relationships
  - ✓ Integrate into existing Aviation Safety controls and environment
➢ Cyber crosses and overlays the various domains (Aircraft, Air Traffic Managements (ATM) , Airports)
➢ Cyber assessments of one domain should be expanded to include other domains

Aviation Systems Information Security Protection (ASISP) Safety Risk Assessment Methodology

Risk Based Decision Making (RBDM) Process for assessing the risks associated with cyber within the aviation eco-system

- ✓ **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**
- ✓ **RBDM is a FAA strategic initiative**
- ✓ **Process based on Systems-Theoretic Hazard Analysis Technique which can be applied to the Aviation Ecosystem**
- ✓ **Compliant with RTCA DO-356A methods**
- ✓ **Sensitive approach to proprietary data**
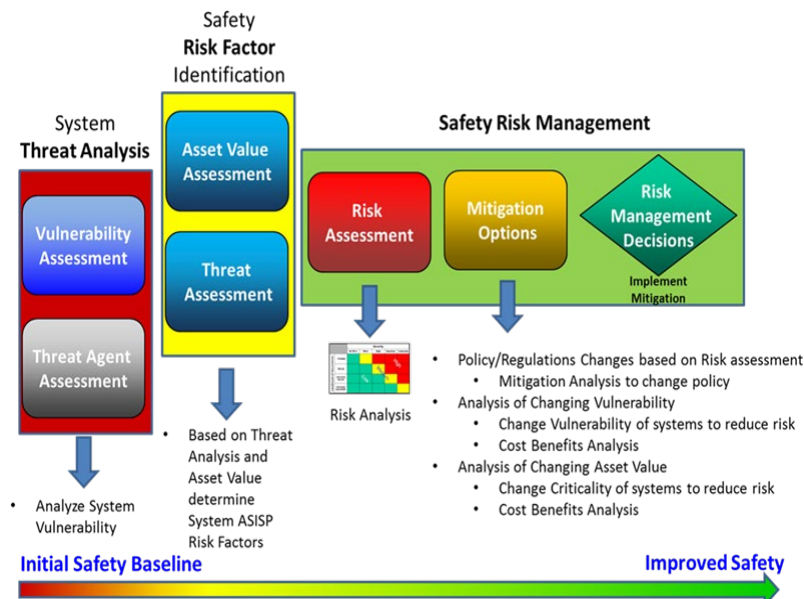
Cyber Safety Commercial Aviation Team (CAT) Preliminary Partners/Structure

US Private Sector

GAMA INTERNATIONAL · ACI NORTH AMERICA AIRPORTS COUNCIL INTERNATIONAL · alpa · Airlines for America We Connect the World · RTCA THE AVIATION GOLD STANDARD SINCE 1935 · BOEING · Astronautics Corporation of America · Collins Aerospace · GE Aviation · Honeywell

US Government

ARP
AVS
ATO
AXE
ANG
AIS

MIT Lincoln Laboratory · ACI · U.S. DEPARTMENT OF HOMELAND SECURITY · DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA

International Private Sector

AVIATION ISAC

International Government

ICAO · OACI · ИКАО · EASA European Aviation Safety Agency

2020 Development Cyber Safety Core Group above
Expected to spiral out and stand up operational Cyber Safety CAT in 2021

10

Cyber Safety CAT Operational Construct

Cyber Risk Based Analysis

ASISP SRA & MIDEP & Industry

Agree on Cyber Risks and proposed mitigations

Set Cyber Safety Priorities

FAA & Industry

Achieve consensus on priorities

Implement Safety Enhancements - U.S.

Influence Safety Enhancements - Worldwide

Integrate into existing work and distribute
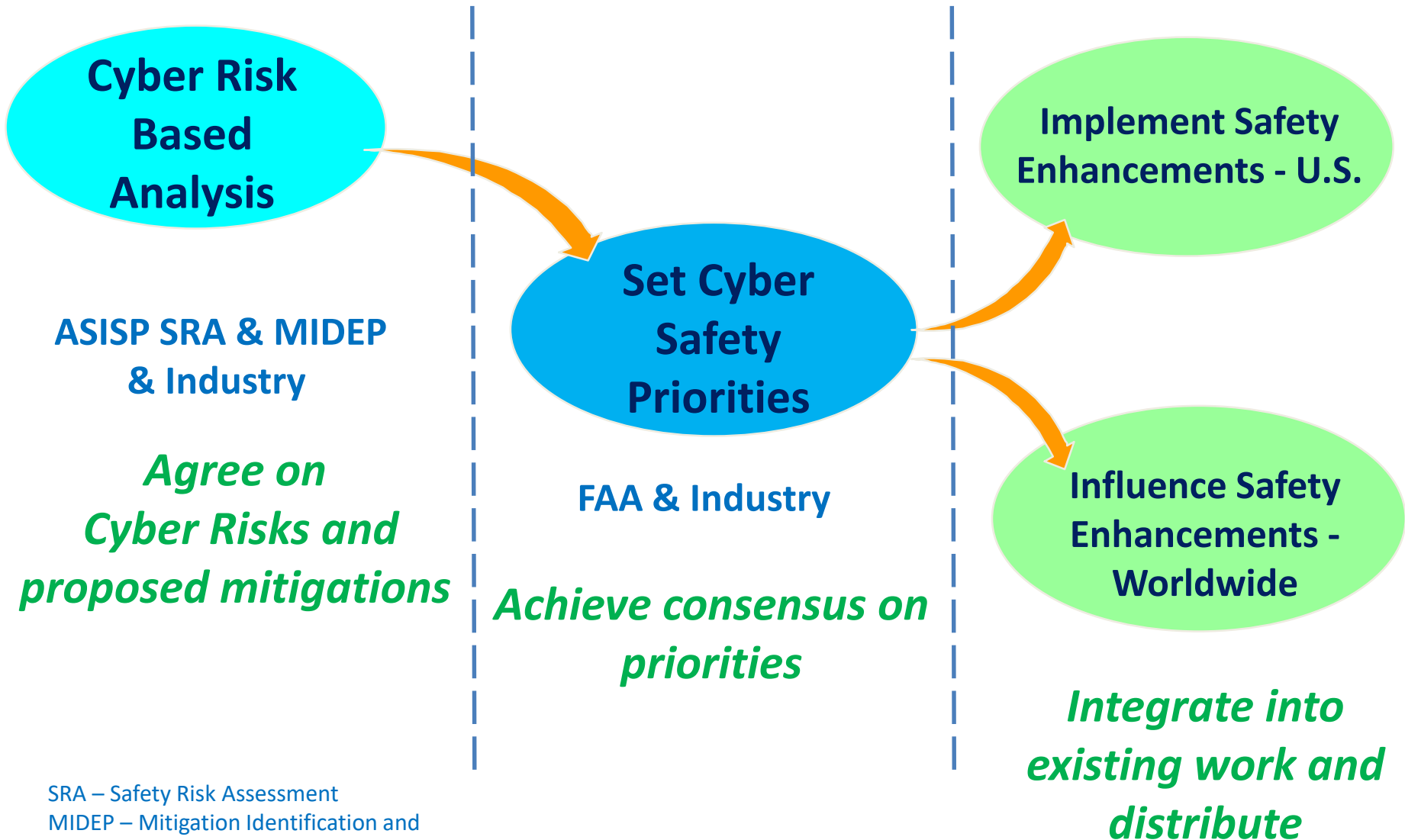
SRA – Safety Risk Assessment
MIDEP – Mitigation Identification and Evaluation Process

11

Why Should "I" Get Involved

Aviation Ecosystem perspective

- **Efficient industry wide resource utilization (cost reduction).**

- **Use Case "end-to-end" perspective that cannot be established independently.**

- **Increase layer of protection across the aviation ecosystem through communication and increased awareness.**

- **Avoid stove-piped assessments.**

- **Provides US based complementary effort to EASA European Strategic Coordination Platform.**

- **Drive solutions for cyber-safety recommendations.**

Summary

- Established cyber safety risk based decision making framework.

- Build upon Safety community success.

- Leveraging existing aviation industry & government partnerships.

- Concept Document is available for review

- Contact Cyber Safety Commercial Aviation Team Leads to get involved.

Contacts
(Cyber Safety Commercial Aviation Team)

Dan Diessner

Boeing Commercial Airplanes – Product Cybersecurity Senior Manager
AIA Civil Aviation Cybersecurity Subcommittee Chair
daniel.j.diessner@boeing.com

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