Overview of Cyber Sa
Cyber Safety Commercial

February 25 2020

Presented to REDAC - Subcommittee for Aviation Safety – SAS
Presented by
Isidore Venetos – FAA Aviation Research Division Cyber R&D Manager
Dan Diessner – AIA Civil Aviation Cybersecurity Subcommittee Chair
Boeing Commercial Airplanes – Product Cybersecurity Senior Manager
ICAO - Trust Framework Use Case & CONOPS Working Group Chair

Evolving Safety Environment

Safety Historically

- 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 Incorporation

- Security culture is getting stronger. Working to have:
  - Cyber Security risks prioritized, and a well understood set of risks and solutions with industry wide approach
  - Well structured Processes & Procedures in place
- Develop record of threat/risks/mitigations
- **Defining "Cyber Safety CAT" community solution**
  - CAST Equivalent for Cyber Safety
  - Solutions based; NOT Regulatory based
  - Consensus-based End-to-End solution sets
- **Need a better managed Cyber-based environment**
  - Better 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
Commercial Aviation Team

Vision

- Data driven risk based collaborative cyber safety decision making.

Mission

- Proactive identification & mitigation of aviation ecosystem cyber safety risks.

Goal

- Reduce U.S. commercial aviation cyber safety risk.
- Work with international partners to reduce cyber safety risk world-wide.

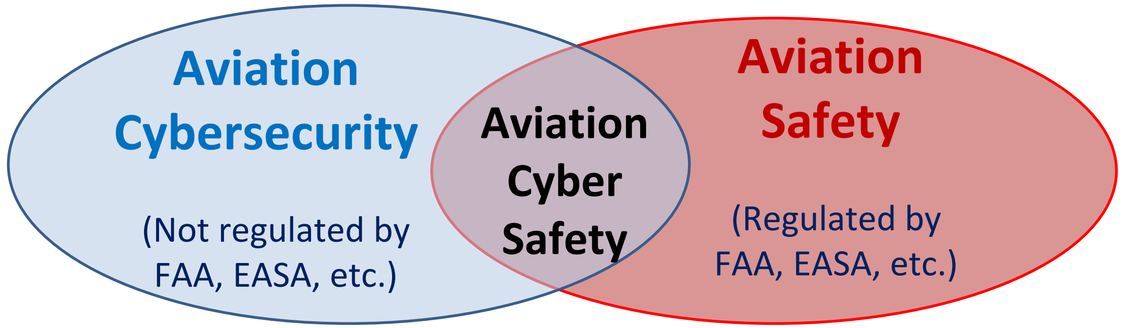
Outcomes

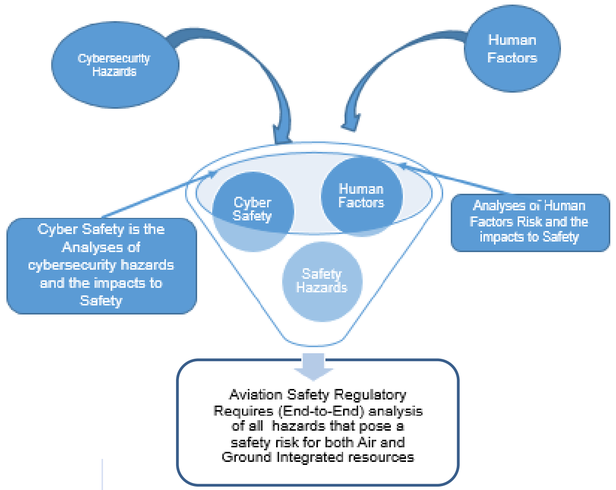
- Identification of risks & actionable ecosystem mitigation recommendations for:
  - Best practices, standards & technology development
  - Aviation Cyber Safety Incident Communications & Response Plans
  - EASA/ESCP Harmonization & ICAO Influence
  - Guidance, policy, and if needed recommendations for regulatory consideration

What is Aviation Cyber Safety Within The Aviation Ecosystem

Cyber Safety hazards include all threat vectors from interconnectivity of the aviation ecosystem that can impact aircraft safety. This includes a focus on the interoperability and efficiency related safety impacts to air/ground resources that have:

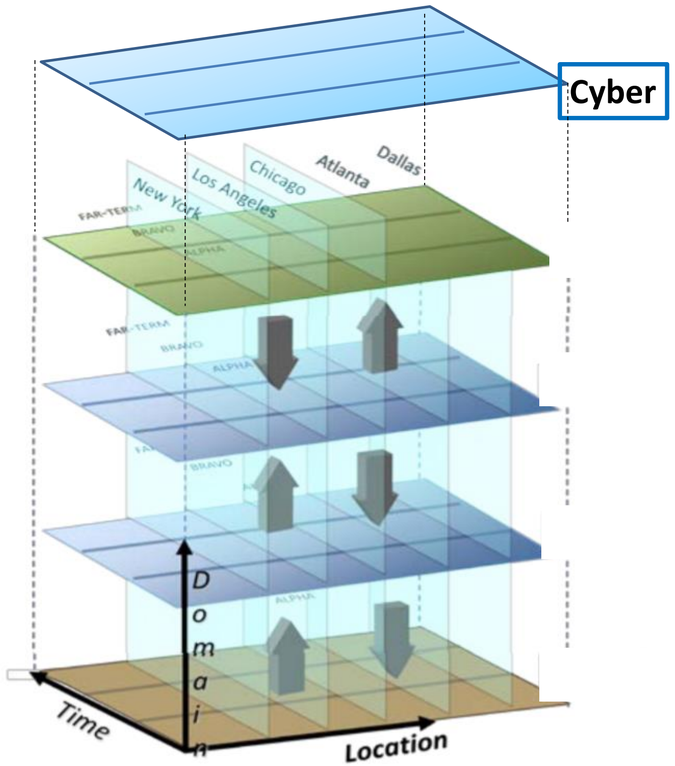
- An ability to directly impact ATM services
  - Impacts to pilot decision making or aircraft control systems (Aircraft)
  - Air-to-Ground Voice and Data
- The ability to directly impact the interoperability between ATM stakeholders responsible for providing ATM critical and safety services
  - Aerodrome (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





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

Cyber Safety CAT Data Management Model

Cyber Safety Commercial Aviation Team

Data Handling Model

Information Detail & Sensitivity

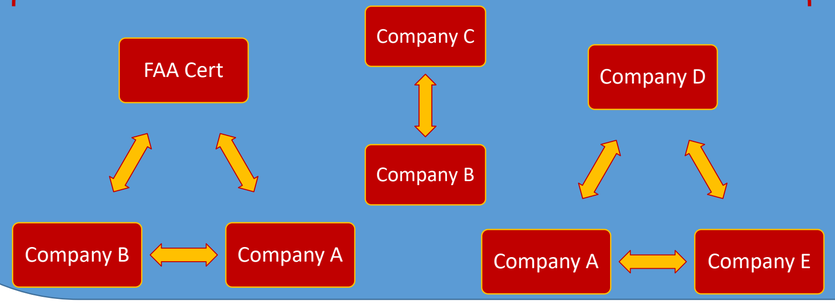
Data Sharing levels

Open
- Shared Openly
- Final Outcomes / Recommendations (US, ICAO, EASA, …)

Sector
- Targeted Aviation Sector Sharing
- High level results

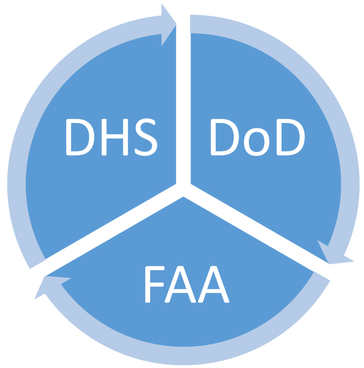
Members
- CSCAT Members
- Working Level Security Data

Limited
- CSCAT Sub-set Only
- Very Limited sharing



Participant Multi-way Limited Proprietary Data

Partners / Data Sharing



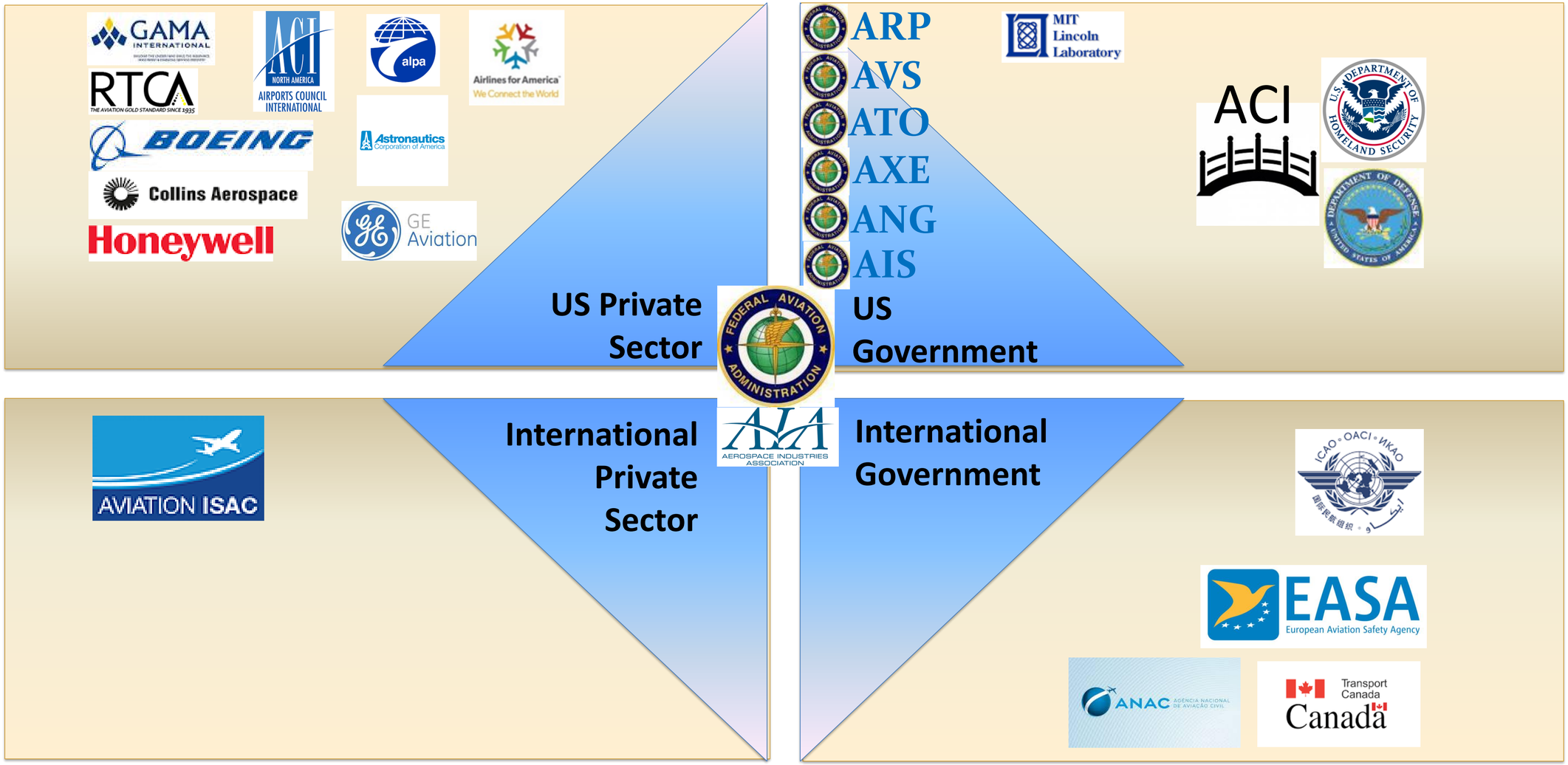
ACI Tri-Chair

NCCIC

Unclassified Data Only

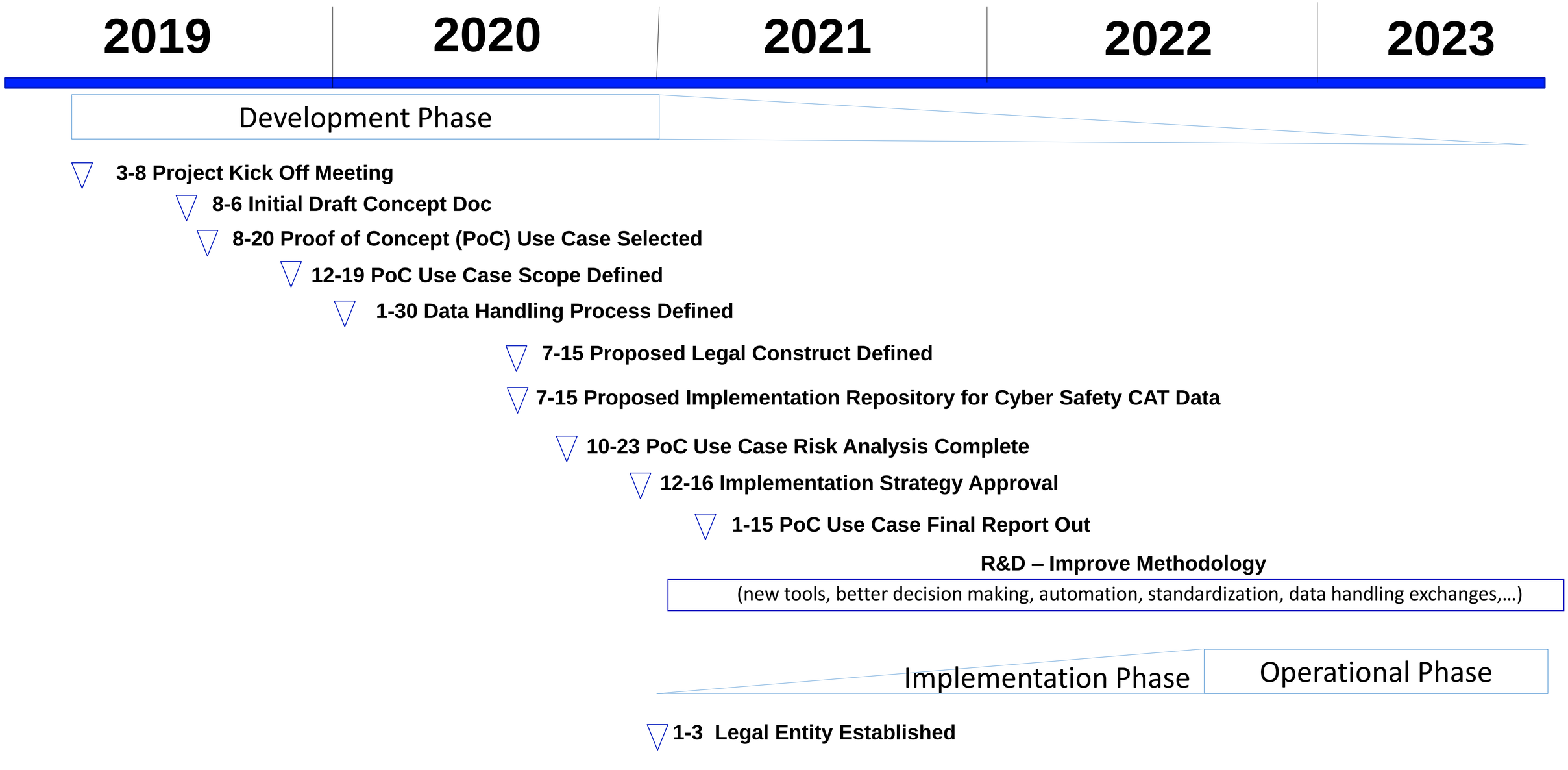
AVIATION ISAC

Cyber Safety Commercial Aviation Team (CAT)
Preliminary Partners/Structure



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

Safety Cyber CAT Tier 0 Plan



Summary

- Established cyber safety risk based decision making framework
- Build upon Safety community success
- Leveraging existing aviation industry & government partnerships
- DRAFT Concept Document is available for review & have begun Use Case Studies
- 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

Susan Cabler

Federal Aviation Administration
Aviation Safety Organization (AVS)
susan.cabler@faa.gov

Questions?