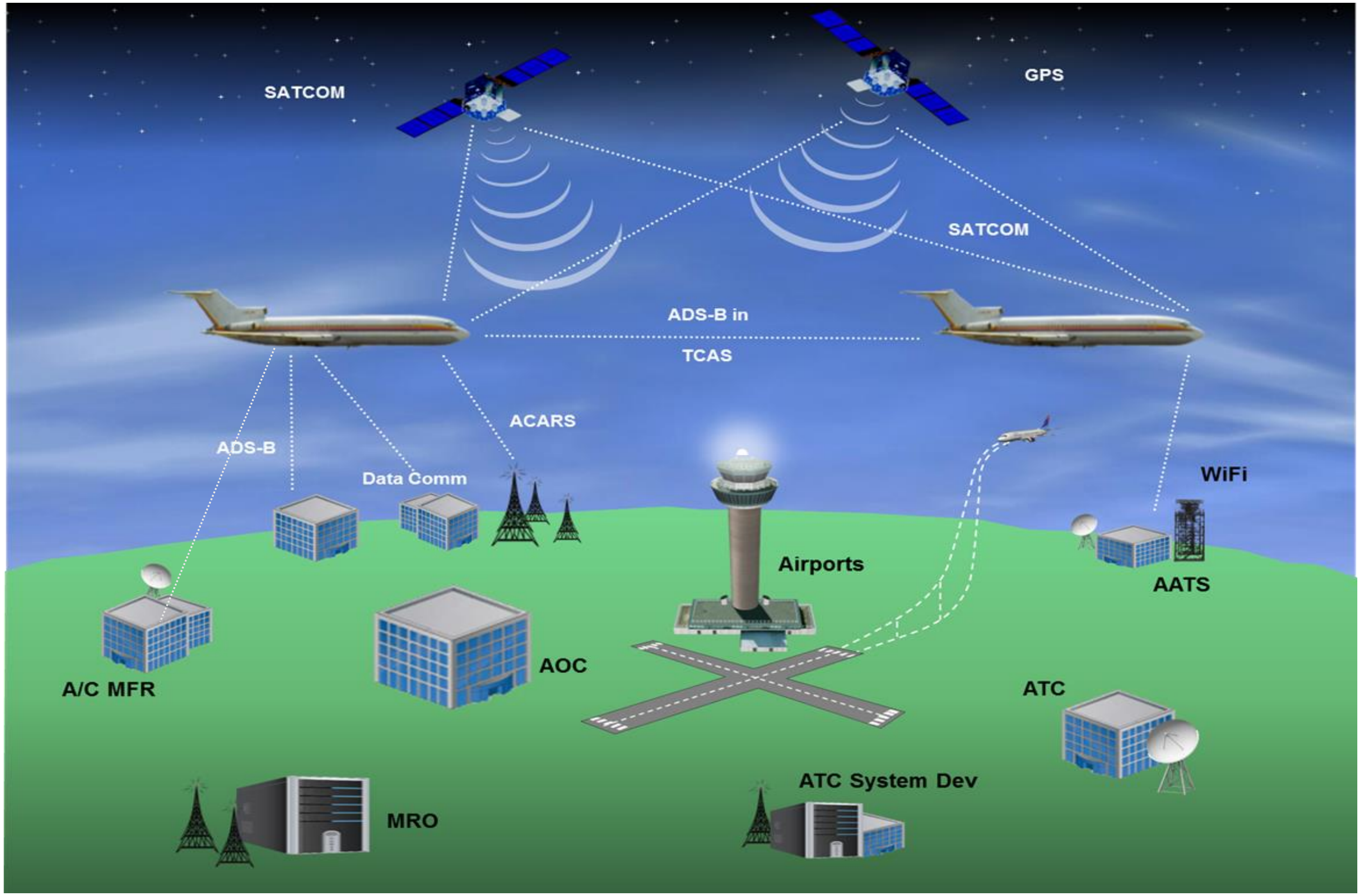
FAA Cyber Strategy and Interagency Coordination Mechanisms

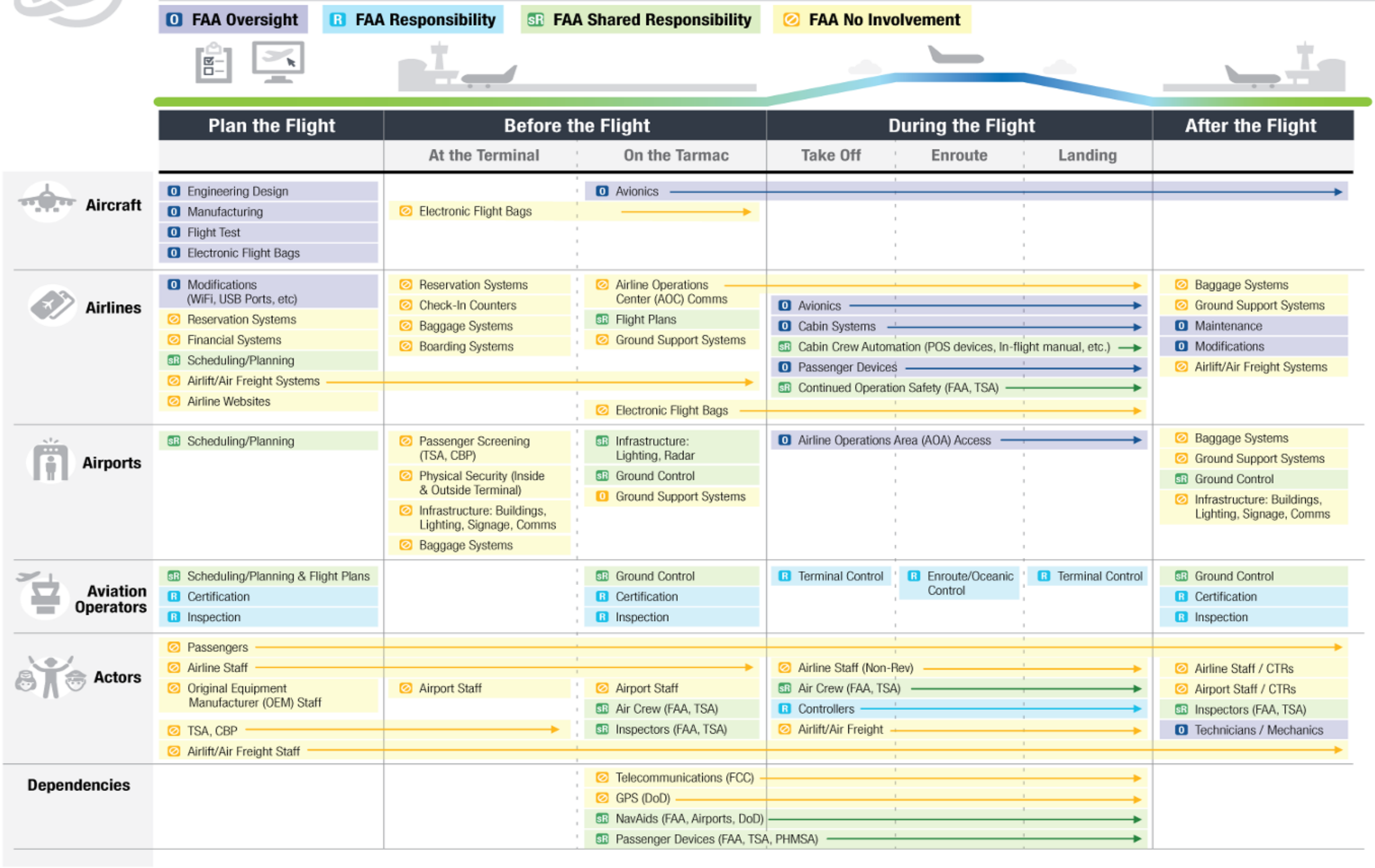
ICAO/ECAC Meeting
Paris, France

Larry Grossman, FAA CISO

Cybersecurity for Aviation involves a range of stakeholders and responsibility is widely distributed



The Aviation Ecosystem: FAA Roles



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 →	O Avionics →				
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) →				

FAA Cyber Community Engagement, ACI and beyond

*The examples listed below are not exhaustive.

U.S. Government

Aviation Cyber Initiative (ACI)

Aviation Government Coordinating Council (AGCC)

Department of Homeland Security (DHS)

- Cybersecurity & Infrastructure Security Agency (CISA)
- Transportation Security Administration (TSA)
- United States Computer Emergency Readiness Team (US-CERT)

Intelligence Community

Private Sector

Aviation Sector Coordinating Council (ASCC)

Aviation Information Sharing & Analysis Center (A-ISAC)

Aerospace Industries Association (AIA)

Airlines for America (A4A)

Airports Council International North America (ACI-NA)

Standards Development Organizations

International

International Civil Aviation Organization (ICAO)

- Cybersecurity Panel and Trust Framework Study Group

Civil Air Navigation Services Organization (CANSO)

International Air Transport Association (IATA)

European Aviation Safety Agency (EASA)

FAA Cybersecurity Strategy

FAA Cybersecurity Strategic Goals 2022-2027

Governance • Vulnerability Management • Security Architecture, Policy, and Standards • Systems and Applications Security • Continuous Diagnostics and Monitoring • Security Operations

Goal 1	Goal 2	Goal 3	Goal 4	Goal 5
Refine and maintain a cybersecurity governance structure to enhance cross-domain synergy	Protect and defend FAA networks and systems to mitigate risks to FAA missions and service delivery	Enhance data-driven risk management decision capabilities	Build and maintain workforce capabilities for cybersecurity	Build and maintain relationships with, and provide guidance to, external partners in Government and industry to sustain and improve cybersecurity in the Aviation Ecosystem

Aviation Cyber Initiative (ACI)

The ACI mission is to reduce cybersecurity risks and improve cyber resilience to support safe, secure, and efficient operations of the Nation’s Aviation Ecosystem.

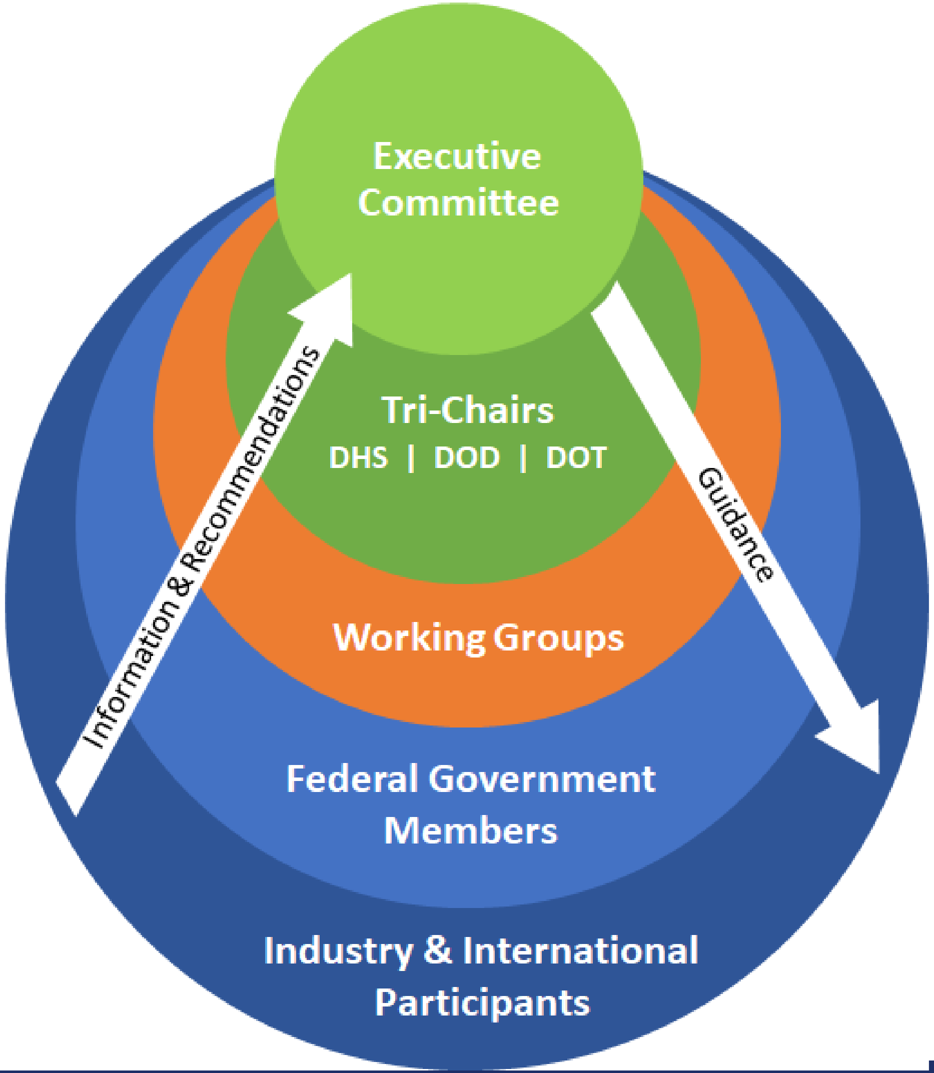
- Charter signed Spring 2019 by DOT, DHS & DOD Secretaries
- Executive Committee (ExCom) made up of:
  - TSA – Stacey Fitzmaurice, Senior Official Performing the Duties of TSA Deputy Administrator
  - DoD – Acting DASD Mr. James Ruocco, Office Undersecretary of Defense Acquisition & Sustainment
  - **A. Bradley Mims, FAA Deputy Administrator**
- Focus is on addressing cybersecurity risk to the Nation’s Aviation Ecosystem to support the National Strategy for Aviation Security (NSAS).

ACI CY22 Priorities

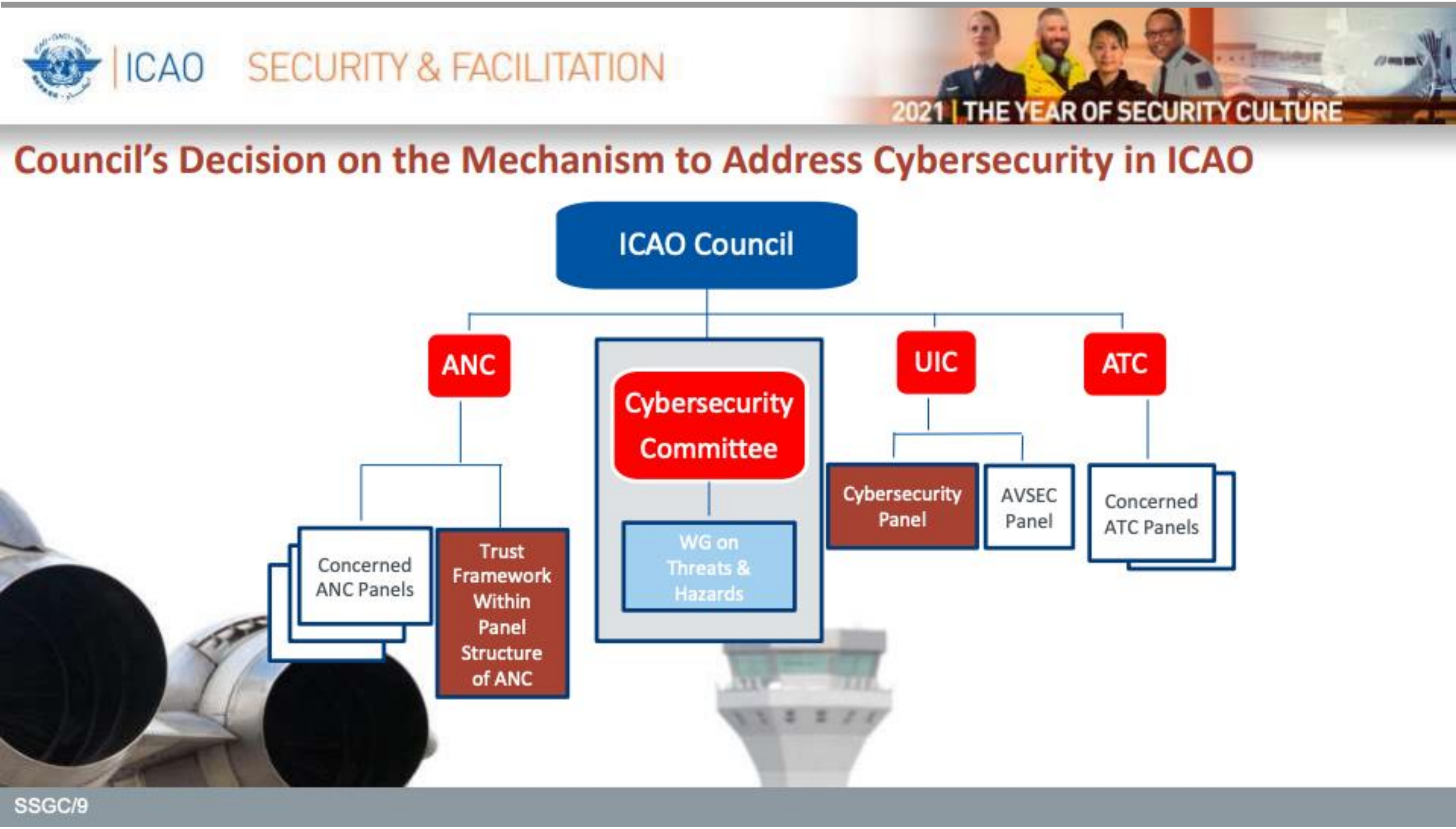
1. Complete established Aviation Cyber Risk Mitigation Initiatives
2. ID Sponsor and Fund integrated GPS detect-and-respond CONOPS for airports and spaceports development
3. Sustain and institutionalize N-FACTOR to support Public-Private Sector Collaboration & Cybersecurity Risk Mitigation
   - Cyber Risk Reduction and Resilience RDT&E Initiatives
   - Co-sponsor and execute 2022 Aviation Cyber Rodeo events
   - Implement Data Sharing Partnership
   - Populate the Resource Guide
4. Conduct Aviation Cyber Tabletop Series (The Wright Brothers Series) Event
5. Conduct initial Interagency Aviation Cybersecurity Training Course
6. Re-establish the Aviation Cyber Threat Working Group (ACTWG)
7. Conduct Annual ACI Summit
8. Track performance metrics for ACI
9. ID & Participate in an Aviation Cyber Risk Assessment for one of six Aviation Ecosystem elements

ACI Community of Interest (COI)

National Strategy for Aviation Security


Executive Committee
Tri-Chairs
DHS | DOD | DOT
Working Groups
Federal Government Members
Industry & International Participants
Information & Recommendations
Guidance

ICAO Cyber Governance



ICAO SECURITY & FACILITATION

2021 | THE YEAR OF SECURITY CULTURE

Council's Decision on the Mechanism to Address Cybersecurity in ICAO

ICAO Council

ANC

Concerned ANC Panels

Trust Framework Within Panel Structure of ANC

Cybersecurity Committee

WG on Threats & Hazards

UIC

Cybersecurity Panel

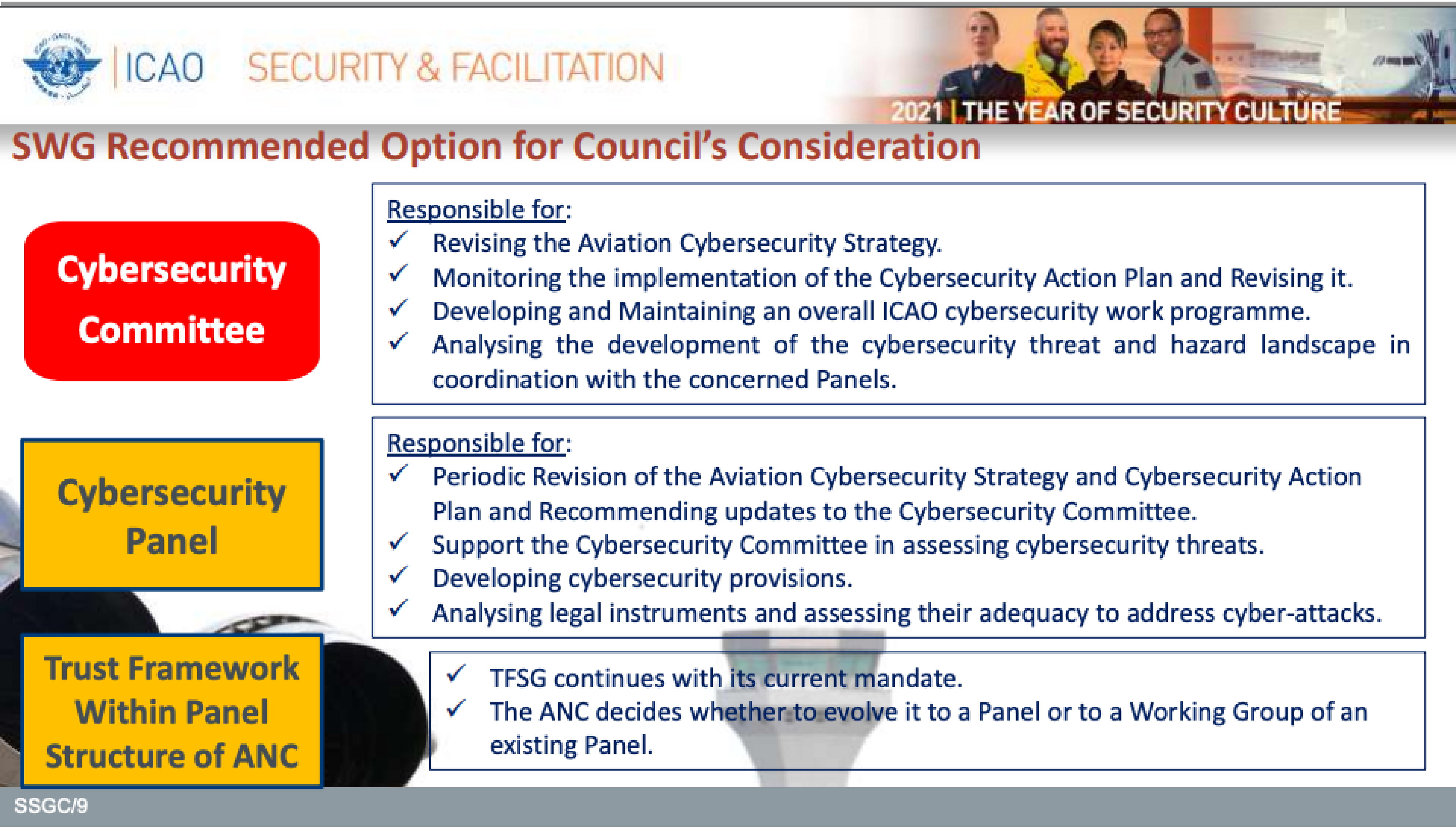
AVSEC Panel

ATC

Concerned ATC Panels

SSGC/9

ICAO Cyber Governance



ICAO SECURITY & FACILITATION

2021 | THE YEAR OF SECURITY CULTURE

SWG Recommended Option for Council's Consideration

Cybersecurity Committee

Responsible for:

- ✓ Revising the Aviation Cybersecurity Strategy.
- ✓ Monitoring the implementation of the Cybersecurity Action Plan and Revising it.
- ✓ Developing and Maintaining an overall ICAO cybersecurity work programme.
- ✓ Analysing the development of the cybersecurity threat and hazard landscape in coordination with the concerned Panels.

Cybersecurity Panel

Responsible for:

- ✓ Periodic Revision of the Aviation Cybersecurity Strategy and Cybersecurity Action Plan and Recommending updates to the Cybersecurity Committee.
- ✓ Support the Cybersecurity Committee in assessing cybersecurity threats.
- ✓ Developing cybersecurity provisions.
- ✓ Analysing legal instruments and assessing their adequacy to address cyber-attacks.

Trust Framework Within Panel Structure of ANC

- ✓ TFSG continues with its current mandate.
- ✓ The ANC decides whether to evolve it to a Panel or to a Working Group of an existing Panel.

SSGC/9

The Global Information Exchange Problem

Aviation expansion without global information protection increases safety and security risks.

- Global aviation is moving from a voice communication system to an automated digital communication system that is currently lacking a mechanism to verify information integrity. Further reliance on voice-based communications will become impractical.
- Global harmonization and policy agreements on digital communication infrastructure are required to provide confidence in digitally exchanged information.
- Need to create an infrastructure that enables a safe, resilient, and secure way to exchange information with multiple global aviation stakeholders in a digital manner that has information verification measures.

The Solution: The International Aviation Trust Framework

- The IATF is implemented by a global organization of the same name to ensure the use of a common policy for network protection and identity. IATF requires 24/7 operational services.

- Founding Members (with ICAO involvement) establish the IATF as a to be determined organizational entity.

- Target audience to join IATF: ICAO (committed to study subject of serving as sponsor) and civil aviation organizations that need to exchange information (ANSPs, airlines, airport authorities, other industry etc.).

- Membership Funded: Membership fees would fund the IATF.

- Common policy: Each of the members' individual security policies are audited and
  mapped to the common policy.

- *The end goal is secure interoperability.*

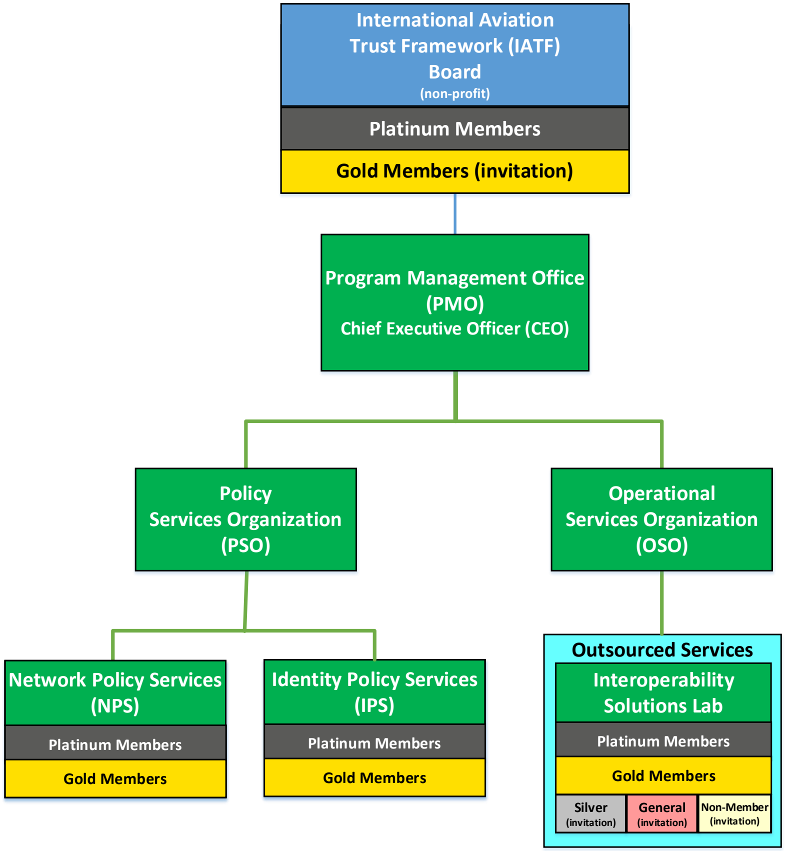
IATF Benefits

Implementing IATF provides members:

- **Confidence that information received is transparent** through harmonized compliance, which creates a baseline understanding of others' systems, the identities in use, and offers the ability to filter what data to accept while being able to attribute information to the actor — good or bad;
- **Interoperability** which offers **reduced operating time and costs**;
- **Reduced administration** due to simplified agreements; and
- Increased automation with **reduced risks.**

All aviation ecosystem participants will benefit from assured compliance with the interoperable, harmonized, legal, technical, and information security requirements that will be verified through independent auditing implemented by the IATF.

IATF Organizational Structure



International Aviation Trust Framework (IATF) Board (non-profit)

Platinum Members

Gold Members (invitation)

Program Management Office (PMO)

Chief Executive Officer (CEO)

Policy Services Organization (PSO)

Operational Services Organization (OSO)

Network Policy Services (NPS)

Platinum Members

Gold Members

Identity Policy Services (IPS)

Platinum Members

Gold Members

Outsourced Services

Interoperability Solutions Lab

Platinum Members

Gold Members

Silver (invitation)

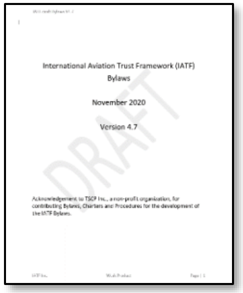
General (invitation)

Non-Member (invitation)

- **Board:** **Platinum member elected Board that provides strategic direction**
- **PMO:** **Day to day management and tiered membership onboarding**
- **PSO:** **Membership driven compliance and requirement interoperability management.**
- **OSO:** **Technical service management for members and interoperability testing lab**

Organizational Documents developed with ICAO

BYLAWS



IATF draft Bylaws V4.7

International Aviation Trust Framework (IATF)
Bylaws

November 2020

Version 4.7

Acknowledgement to TSCP Inc., a non-profit organisation, for contributing Bylaws, Charters and Procedures for the development of the IATF Bylaws.

IATF Inc. Work Product Page | 1

- **Bylaws:** **The Bylaws establish IATF’s management structure and the roles and responsibilities of its Board and Members. Define IATF’s procedures, dispute resolution processes, and specify how IATF conducts its affairs**

Legal Agreements

IATF MTFSA Version 2.3

International Aviation Trust Framework (IATF)
Master Trust Framework Service Agreement (MTFSA)
Version 2.3
June 2021

TSCP Inc. Work Product 1 | Page

- **MTFSA:** **Unified legal agreement between IATF and Members consisting of terms and conditions, liabilities, indemnifications, warranties and privacy requirements**

Managed Technical Requirements

DISTRIBUTION: ICAO/IATF
STATUS: DRAFT

ICAO

X.509 Certificate Policy
for the
International Aviation Trust Framework (IATF)
Certification Authority
Version 0.92
June 04, 2021

- **Managed Technical Requirements:** **for Trusted Identities, Identity Policy, Trusted Networks and Network Policy**