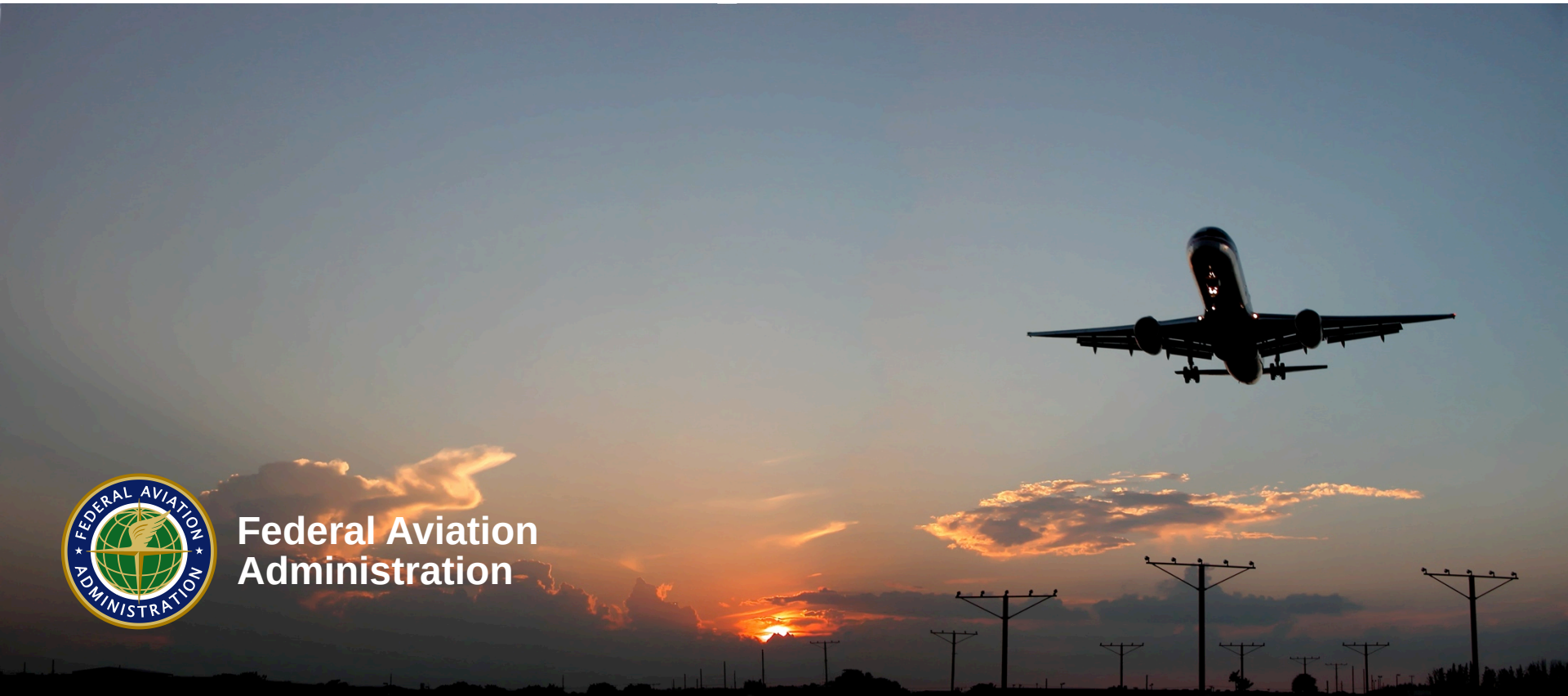
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

ATO Cybersecurity Group

Date: October 20, 2020



ATO Cybersecurity Group

Secure ATO systems and services from existing and evolving cybersecurity threats

Functions

- ***FISMA Compliance/Risk Management***
- ***Support for NAS Cyber Operations***
- ***Enterprise Security Strategy, Partnerships, and Governance***
- ***Establishing Enterprise ATO Security Services***

ATO Cybersecurity Principles

ATO Cybersecurity Group Guiding Principle

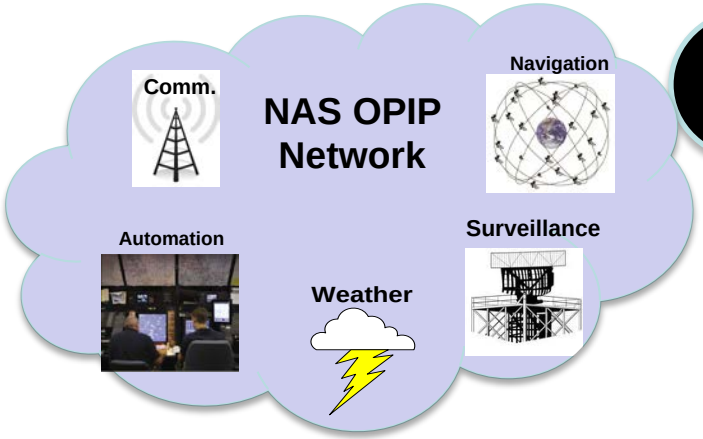
ATO Cybersecurity Group will adapt to challenges by balancing aviation/aerospace safety and efficiency through leveraging cybersecurity processes and technology, maintaining employee and customer relationships, being innovative leaders to minimize risk exposure.

ATO Cybersecurity Group Principles

Business Principles

- Authorization management aligns safety assessments, security posture, and cybersecurity oversight in accordance with Risk Management Framework
- Cybersecurity technology integration supports a path to emerging ATO innovation
- Securing the NAS thru ATO cybersecurity prescriptive governance promotes safety and efficiency
- Centralized Risk and Remediation management is essential to the comprehensive analysis and prioritization of cyber risks to reduce operational impacts

ATO Cybersecurity Group Principles



Critical Infrastructure & Resiliency Principles

- NAS critical infrastructure is Operational Technology (OT) operating as Industrial Control Systems (ICS)
- Data criticality trust levels must provide segmented service flows
- Boundary security controls must implement service segmentation
- ATO non-critical infrastructure must adhere to Information Technology (IT) standards, guidelines and service level assurance

ATO Cybersecurity Group Principles

Enterprise Solution Principles

- Enterprise solutions must promote effective use of FAA resources to optimize core ATO cybersecurity strategies
- Solutions must limit risk exposure while balancing resiliency, complexity, and operability

ATO Cybersecurity R&R

Cybersecurity Roles & Responsibilities

U.S. DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION

ORDER 1370.121

National Policy

Effective Date: 12/23/16

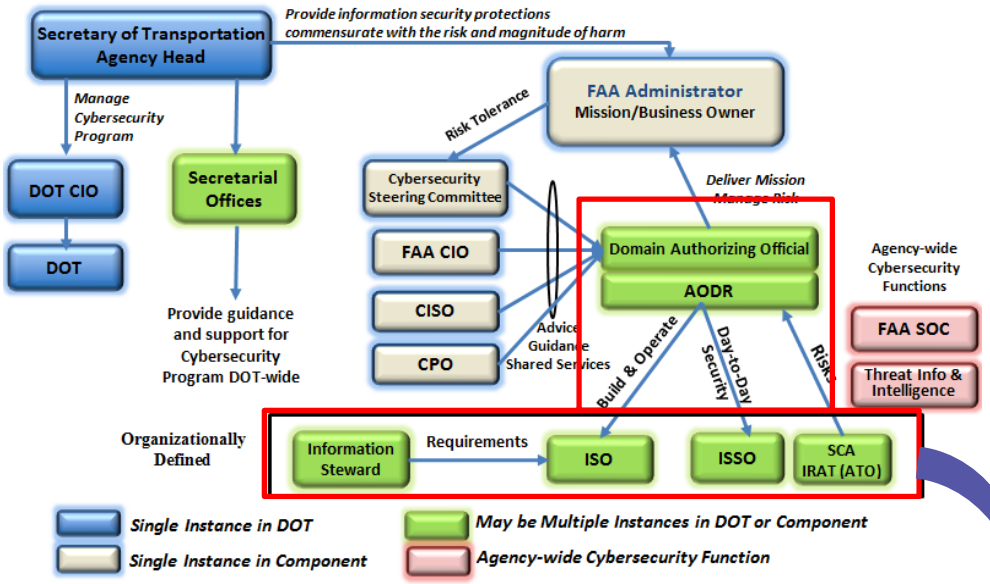
SUBJ: FAA Information Security and Privacy Program & Policy

Consistent with the Federal Information Security Modernization Act of 2014 (FISMA), Office of Management and Budget (OMB) Circular A-130, Federal policies, related laws, regulations, and other mandatory guidance and standards related to information security, information assurance, network security, and privacy, the Federal Aviation Administration (FAA) must protect the confidentiality, integrity, and availability of all FAA information and information systems.

The FAA maintains information and information systems that support the Agency, aviation safety and security, and the National Airspace System (NAS). FAA information systems rely on comprehensive information security to insure proper operation and protect against unauthorized access. This order establishes the FAA National Information Security and Privacy (IS&P) Program and Policy. The FAA Chief Information Security Officer (CISO) developed this FAA National IS&P Program and Policy through a collaborative effort involving cross-organizational security representatives from all FAA Lines of Business (LOB) and Staff Offices (SO).

The core component of the FAA IS&P Program and Policy is the formal adoption of the Department of Transportation (DOT) Cybersecurity Compendium, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Presidential directives, Executive Orders, OMB Memorandums, Department of Defense (DOD) requirements (as appropriate), Department of Homeland Security (DHS) cybersecurity guidelines, Federal Risk and Authorization Management Program (FedRAMP), other Federal policies and guidance, and future revisions.

This policy allows the FAA to meet organizational and mission requirements as well as FAA strategic objectives. It specifies the Agency-wide minimum security and privacy requirements for all FAA systems and defines roles and responsibilities for key cybersecurity positions.



FAA Order 1370.114 requires organizations to define cyber roles and responsibilities at the Authorizing Official (AO) level and below

Cybersecurity Roles & Responsibilities

ATO Cybersecurity R&R Order planned for release in FY21

U.S DEPARTMENT OF TRANSPORTATION
FEDERAL AVIATION ADMINISTRATION
Air Traffic Organization Policy

ORDER
JO 1370.XXX

Effective Date:

xx/xx/2020

SUBJ: Air Traffic Organization (ATO) Cybersecurity Roles and Responsibilities

Federal Aviation Administration (FAA) cybersecurity roles and responsibilities are stated in FAA Order 1370.121, FAA Information Security and Privacy Program & Policy, as amended. This Order defines and tailors the cybersecurity roles and responsibilities for the ATO.

Teri L. Bristol
Chief Operating Officer (COO)
Air Traffic Organization (ATO)

ATO Cybersecurity Roles

- ATO Authorizing Official
- ATO Authorizing Official Designated Representative (AODR)
- ATO Cybersecurity Executive (ACE)
- ATO Cybersecurity Steering Committee (ATO-CSC)
- ATO Cybersecurity Group (ACG) Manager
- ACG Information System Security Officer (ISSO)
- ACG Privacy Officer
- ACG System Assessor
- ATO NAS Cybersecurity Operations (NCO)
- ATO Information System Owner (ISO)

Cybersecurity Roles & Responsibilities

- *Clarity*
- *Ownership*
- *Advocacy*
- *Establishment*
- *Management*
- *Implementation*
- *Operations*
- *Remediation*
- *Maintenance*

ATO Executive Roles (Owners)

ATO – CSC (Advocates)

ACE/ACG Cyber Program (Management and Operations)

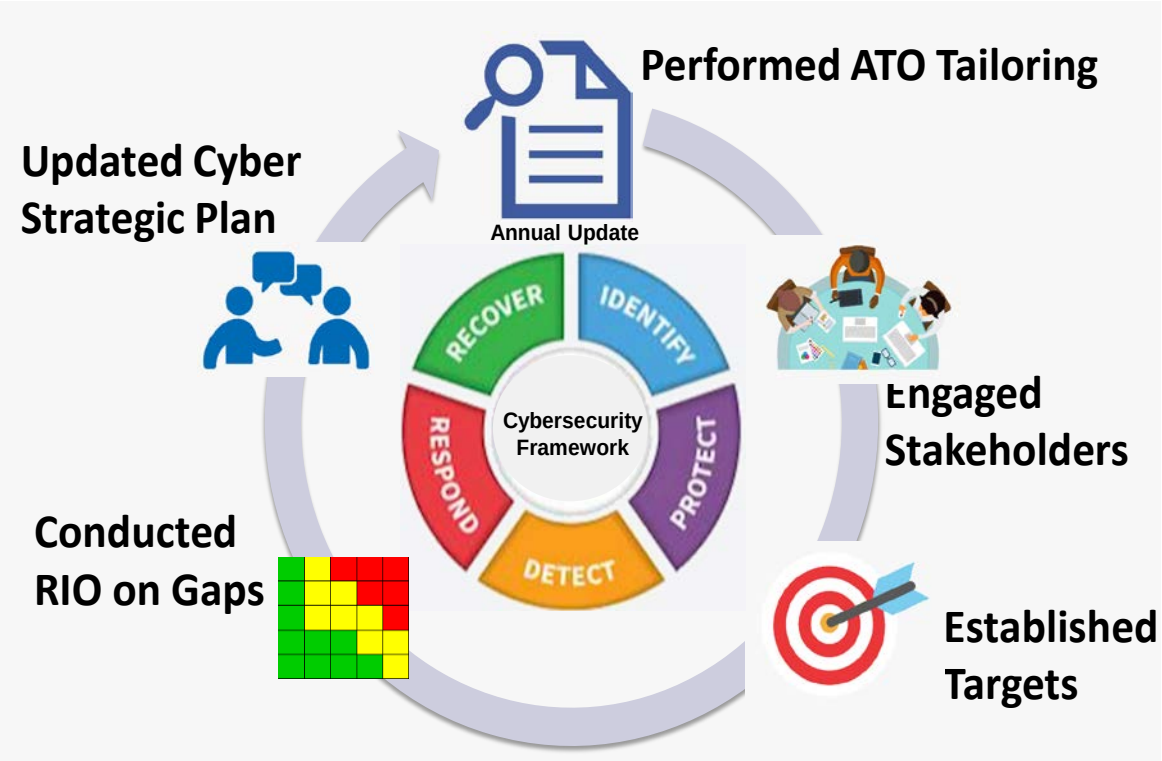
Program Responsibility (ISO) (Implementation and Maintenance)

ATO FY21 Cyber Strategic Plan

Federal Aviation Administration

FY21 Cybersecurity Strategic Plan

ATO Cybersecurity Framework



The CSF is a detailed assessment and analysis tool to:

1. Describe the current ATO cybersecurity posture
2. Describe a target state for cybersecurity maturity
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process
4. Assess progress towards the target state
5. Communicate among internal and external stakeholders and generate the ATO Cybersecurity Strategic Plan

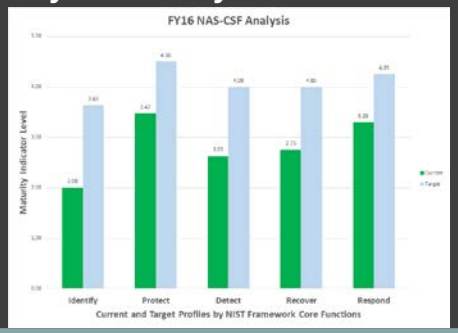
FY21 Cybersecurity Strategic Plan

Governance Drivers
- NIST 800 53
- NIST 800 39
- NIST 800 82
- OMB 14 03
- GAO/OIG Audits

Operational Drivers
- Evolving Cyber Threat
- Cyber Intelligence
- NAS Requirements
- Contingency Planning
- Cyber Incidents
- Future Requirements

Risk, Issues and Opportunities Analysis

NAS Cybersecurity Framework - Gaps



Prioritized Gaps

Critical Infrastructure Enhancements

Strategic Plan
- Vision
- Mission
- Enterprise Security Approach
- Operationally Focused Security

FY21 Cybersecurity Strategic Plan

Strategic Goals
1. Centralized Risk Management
2. Cybersecurity Enterprise Architecture
3. Cybersecurity Enterprise Solution/Development
4. Operational Integration
5. Workforce Development/Awareness
6. External Engagement

Business Plan Targets
1. Conduct security testing on 80% of FISMA Reportable Systems
2. Complete 80% of SARs on FISMA Reportable Systems
3. Establish RMAG operational capability at the WJHTC
4. Participate in FAA Order 1370.121A restructure