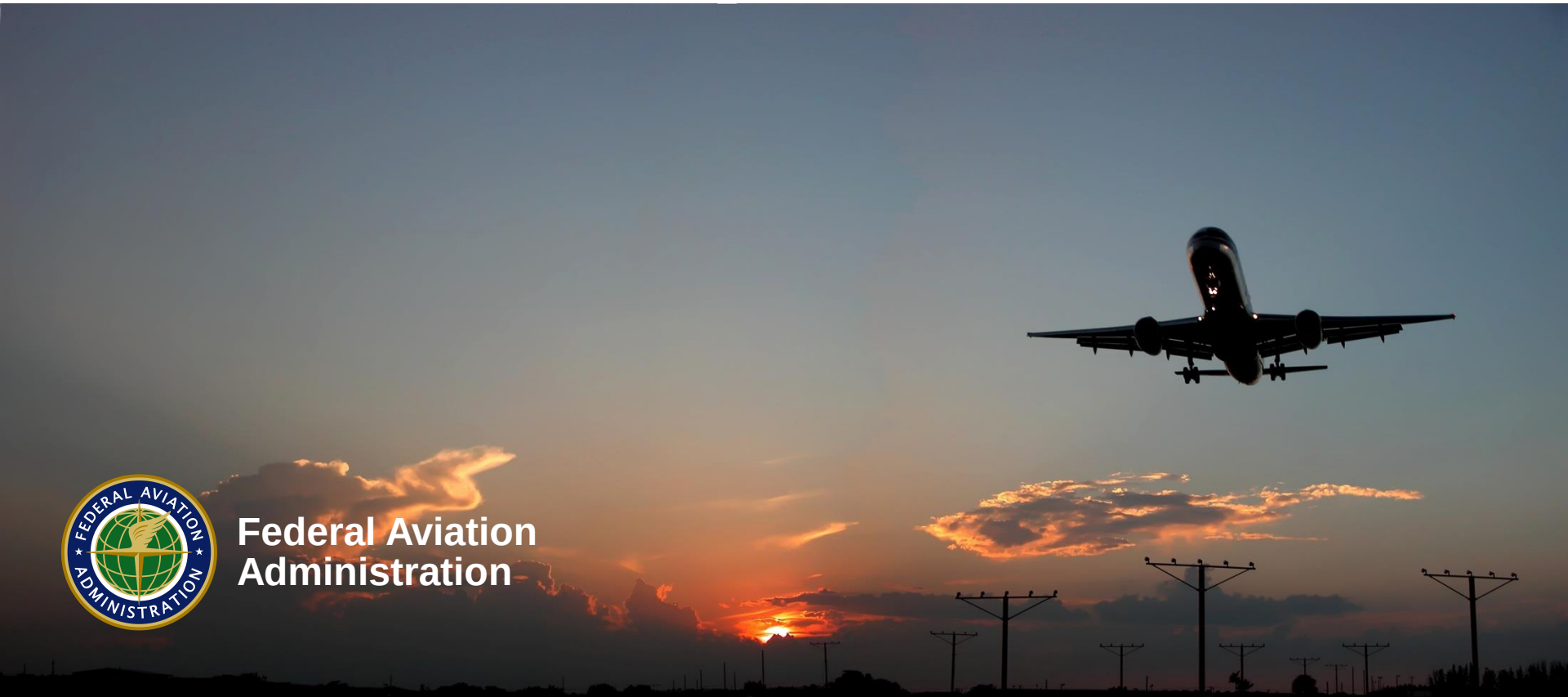
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

Acquisition Management System (AMS) Information System Security (ISS) Assessments

Date: October 20, 2020



ATO Cybersecurity Group (ACG) Information Security Guidance for System Acquisition (ISGSA)

- **Mission Statement**
  - To integrate ISS at each system acquisition (JRC) milestone to ensure Information System Owners (ISO) and Programs understand and include ISS requirements throughout a system's acquisition.
- **The Information Security Guidance for System Acquisition (ISGSA) facilitates, through the ISS Assessments, the:**
  - Identification of ISS risk for use by the Joint Resource Council (JRC);
  - Preparation of security cost and benefit factors;
  - Prioritization of common controls.
- **Team Functions:**
  - The Air Traffic Organization (ATO) Cybersecurity Group (ACG) Program Control & Governance maintains the ATO-tailored AMS ISS templates.
  - Information Systems Security Officers (ISSO) guide programs through the ISGSA process.
  - The ATO Cybersecurity Group Manager (AJW-B4) reviews and provides recommendation for concurrence for submitted ISS completed templates.

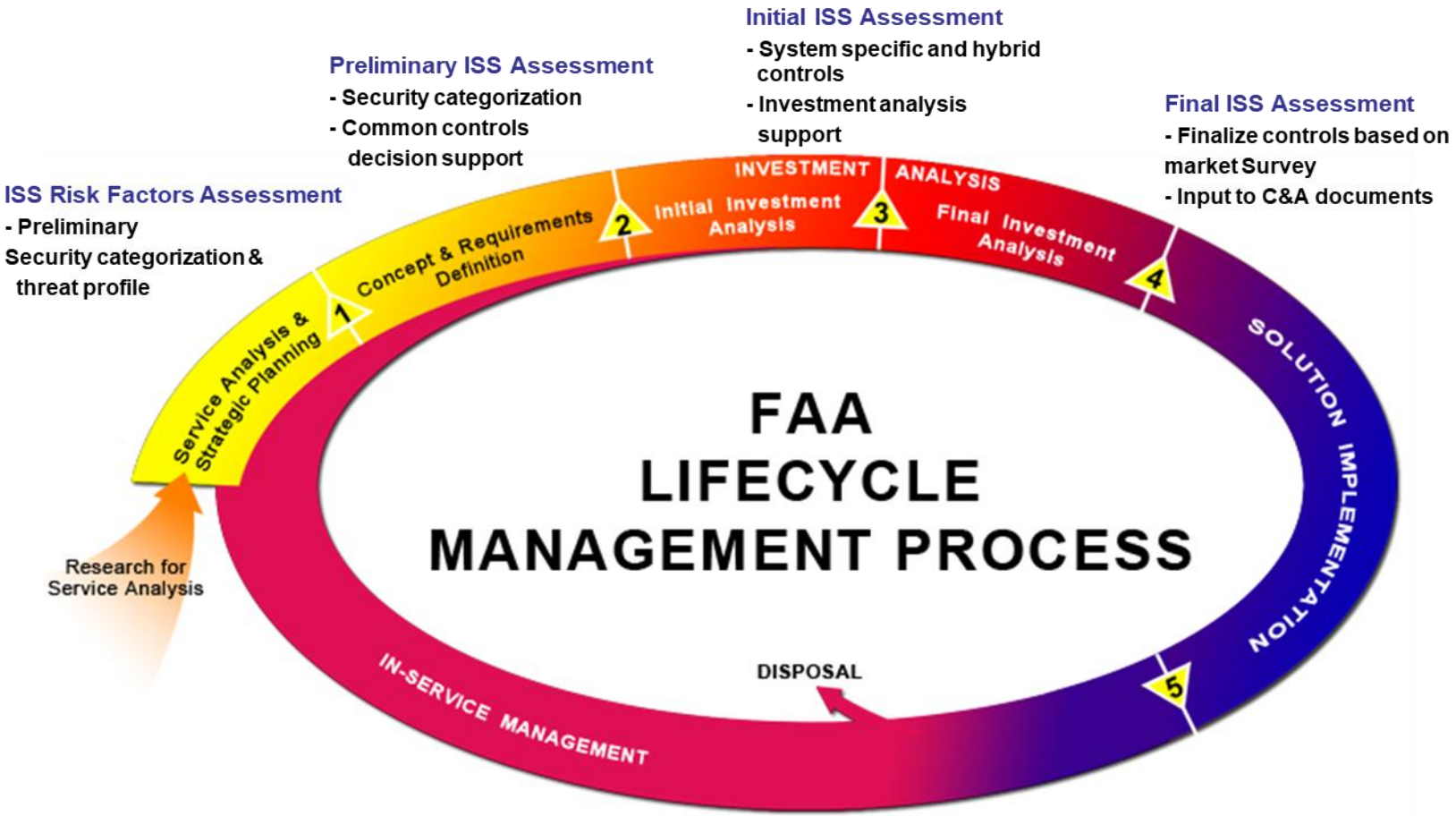
Functional Area of Responsibility

- **ATO Cybersecurity Group Manager**
  - Review & provide recommendation for concurrence for submitted ISS templates
- **ISO**
  - Coordinate ISS meeting with ISSO to discuss investment
  - Perform assessment & complete template
- **ISSO**
  - Guide ISO/Program through the ISGSA process
  - Ensure completed template complies with ISS policy

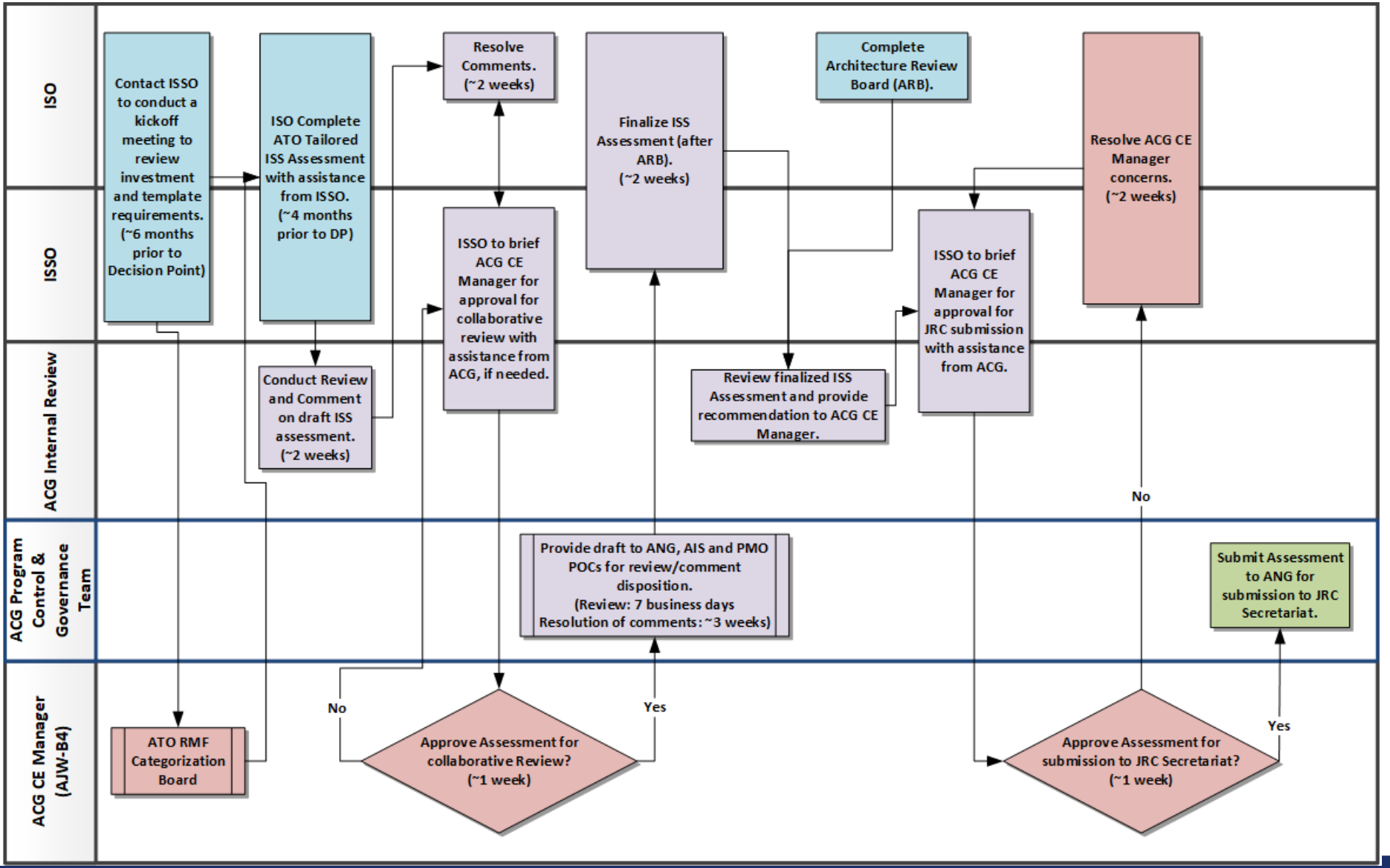
By reviewing ISS requirements, proposed architectures, users, data types, and integration of enterprise services at each JRC milestone enhances the cyber hygiene of the final system.

ISGSA

Security risk assessments supporting information security requirements will be done earlier and will better support implementation and security authorization/documentation.



ISGSA Process



1. ISS Risk Factors Assessment Summary (CRDR)

- **Prospective Capability Purpose:**
  - What customer needs will the capability satisfy?
- **Capability Description**
  - Purpose of the investment (ex. traffic flow mgmt.)
  - Architecture Diagram (ex. boundaries and connections)
  - Environment (ex. manned, air traffic facility, NAS)
  - Users, Operators (FAA employees, remote maint.)
  - Applicable ISS policies (ex. 1370.121)
- **Security Categorization**
  - Information types (mission based, mgmt., other)
  - Provisional Confidentiality, Integrity, Availability of each type

2. Preliminary ISS Assessment Summary (IARD)

- **Purpose:**
  - Update to ISS Risk Factors Assessment as necessary
  - Determine baseline of security controls.
- **Capability Description**
  - Architecture Diagram (ex. boundaries and connections)
  - Applicable ISS policies
- **Security Categorization**
  - Determines the Baseline of NAS-tailored security controls
- **Identify Common (or Inherited) Controls**
  - ex. ASH for PE; NESG; NCO; FTI
- **Cost Estimate**
- **ISS Benefit Estimate**
- **Plans of Actions and Milestones (POAMs)**
  - For Sustainments and Tech Refreshes, address current POAMs.
  - For New/Replacement systems, address POAMs for legacy systems. ACG must review the SIR and contract requirements.

3. Initial ISS Assessment Summary (IID)

- **Purpose:**
  - Update to Preliminary ISS Assessment as necessary
  - Main product of assessment is fully tailored set of security controls
- **Capability Description**
  - Architecture Diagram (ex. boundaries and connections)
  - Applicable ISS policies
- **Security Categorization**
- **Identify Common (or Inherited) Controls**
  - Identified in the NAS-tailored security controls spreadsheet
- **Tailoring Controls**
  - Tailor controls for the system by completing the requirements matrix
- **Cost Estimate**
- **ISS Benefit Estimate**
- **Plans of Actions and Milestones (POAMs)**
  - For Sustainments and Tech Refreshes, address current POAMs.
  - For New/Replacement systems, address POAMs for legacy systems. ACG must review the SIR and contract requirements.

4. Final ISS Assessment (FID)

- **Purpose:**
  - Update to Initial ISS Assessment as necessary.
- **Capability Description**
  - Architecture Diagram (ex. boundaries and connections)
  - Applicable ISS policies (ex. 1370.114)
- **Security Categorization**
- **Identify Common (or Inherited) Controls**
- **Tailoring Controls**
  - Tailor controls for the system by completing the requirements matrix
- **Cost Estimate**
- **ISS Benefit Estimate**
- **Plans of Actions and Milestones (POAMs)**
  - For Sustainments and Tech Refreshes, address current POAMs.
  - For New/Replacement systems, address POAMs for legacy systems. NISG must review the SIR and contract requirements.