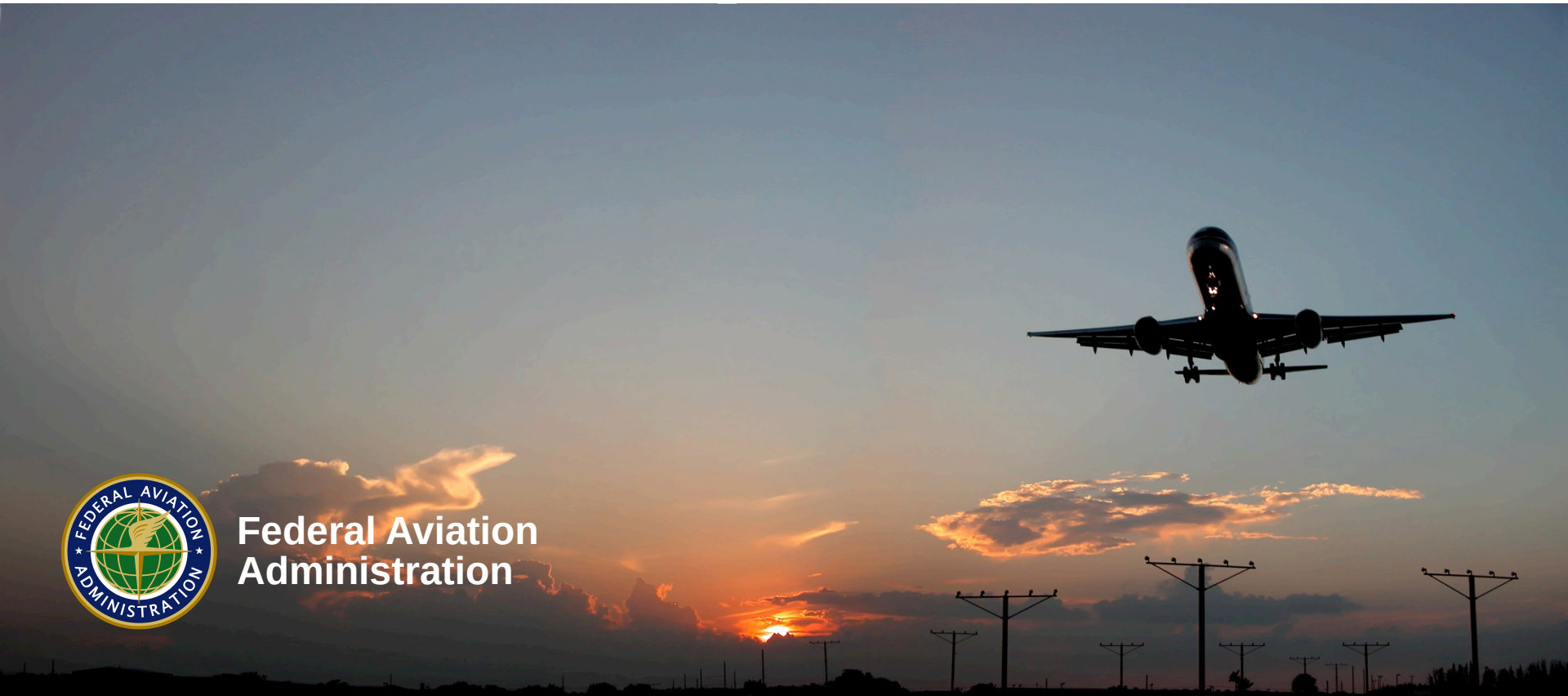
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

Cyber Testing

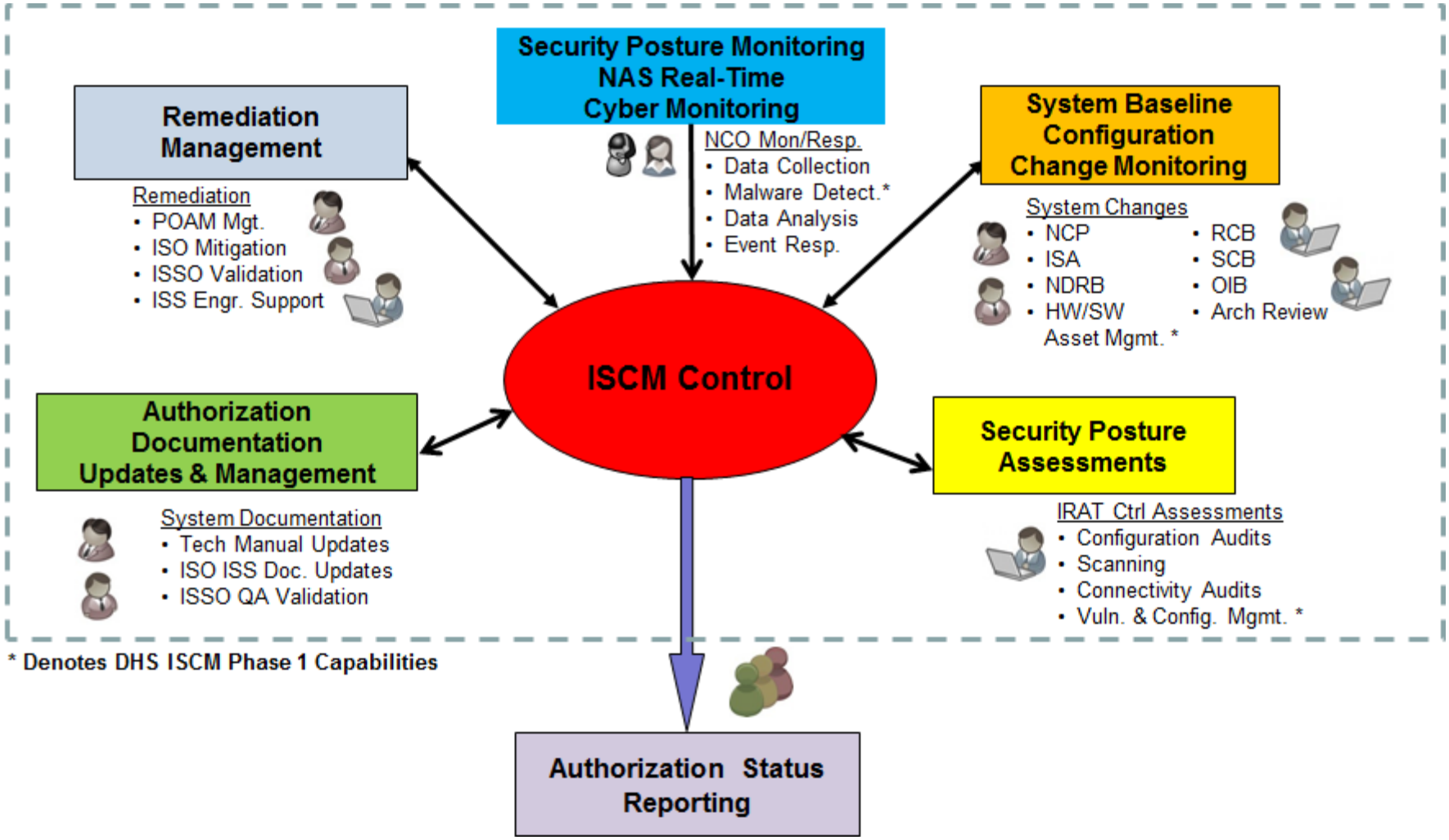
Date: October 20, 2020



Cyber Testing (CT)

- **The CT Mission is to conduct independent security and vulnerability assessments and report on the security posture of all ATO systems and assets by testing and evaluating compliance to security requirements, maintain the NAS Cyber Engineering Facility (NCEF), and to support the NAS Cyber Monitoring System (NCMS) utilized by the NCO.**
- **The CT roles include:**
  - Conduct vulnerability and compliance scanning and penetration testing on ATO systems
  - Serve as the independent assessor to determine the actual system's security posture and risks associated with each ATO system
  - Develop and document in Security Assessment Reports (SARs) vulnerabilities and risks to assist the AO in authorization decisions
  - Maintain the NCEF to support testing and ACG tools, including NORA, ATOM, and IRIS
  - Conduct testing on new assets including edge devices such as taps
  - Maintain the NCMS and on-board ATO systems to the NCMS

ISCM Process



IRAT Functional Area of Responsibility

- **IRAT coordinates security assessment activities with ISSOs, as one step of the overall authorization process, in accordance with the Authorization and ISCM Master Schedule,**
- **IRAT functions and process include:**
  - Planning, coordinating and conducting security testing to evaluate security vulnerabilities and compliance with security requirements
  - Conducts on-site testing at operational, labs and/or support-level facilities to collect actual security configuration information
  - Evaluating security documentation, processes, and procedures to ensure system's security mechanisms meet security requirements
  - Analyzing security testing results to identify vulnerabilities and risks in each systems security posture.
  - Prepare and submit system Security Assessment Reports (SARs) to assist the AO in authorization decisions

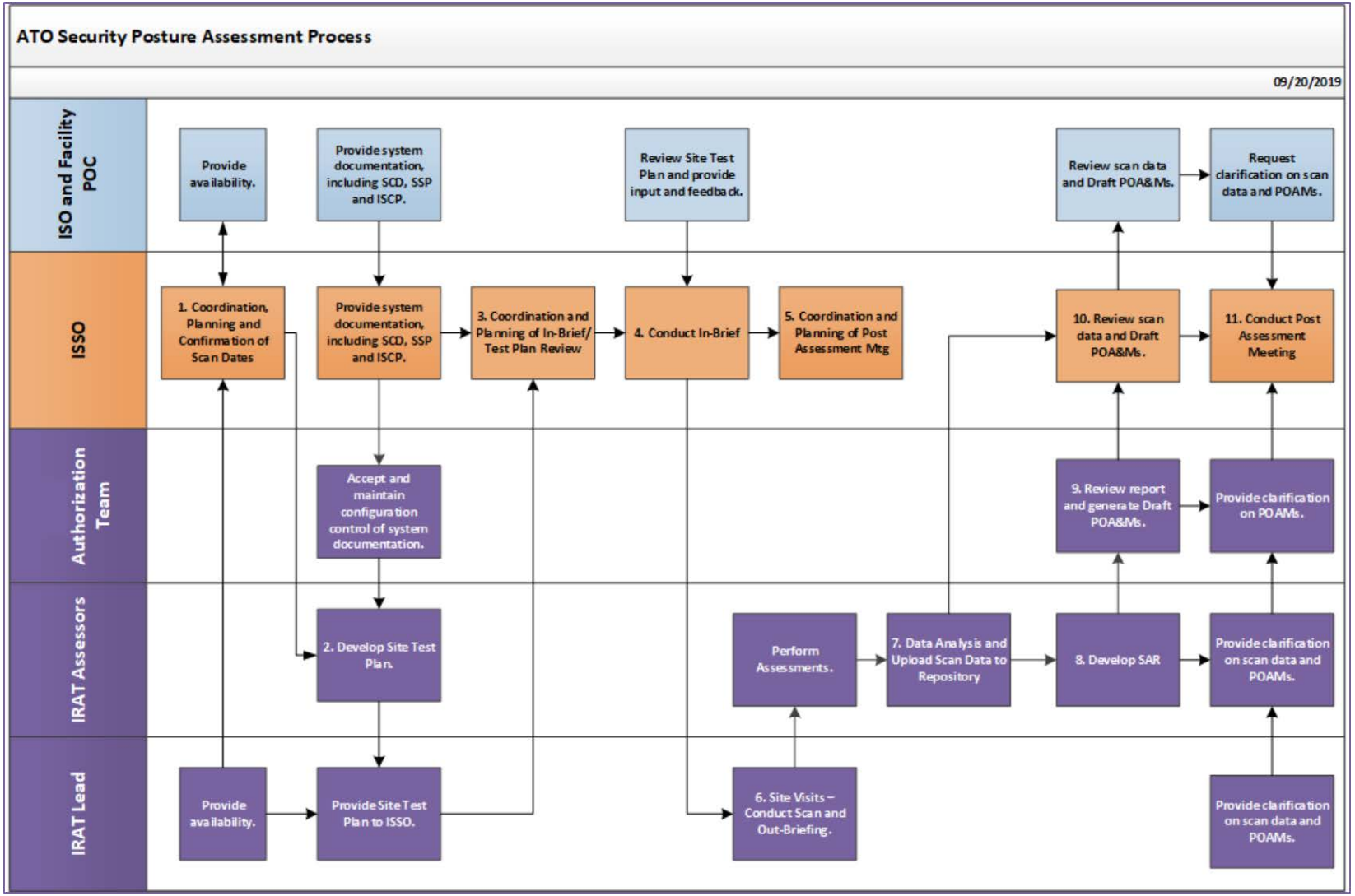
ISCM – Security Posture Assessments

- **Conducted by the Independent Risk Assessment Team (IRAT)**
- **New systems are assessed against the whole set of ATO Security Requirements**
- **Systems in the continuous monitoring cycle are assessed against a subset of security requirements**
- **Output of the security assessment is the Security Assessment Report**
  - **The SAR is a milestone on the ATO ISS Authorization and ISCM Schedule**

ATO ISS Requirements

- **ATO ISS Requirements**
  - **ATO system ISS requirements are identified in the ATO ISS Requirements document**
    - **Tailored for the ATO environment based on NIST SP 800-53 Rev4**
    - **Contains requirements for systems with High, Moderate and Low FIPS-199 Security Categorizations (SCs)**
    - **Available on the ATO ISS Program Website**
- **All ATO systems are assessed against the ATO requirements**

Security Posture Assessments Process



Security Posture Assessments Process

- **ISSOs conduct the following activities as part of the Security Posture Assessment Process**
  - Coordination, Planning, and Confirmation of Scan Dates for each System
  - Coordination and Planning of In-Brief/Test Plan Review
  - Conducting In-Brief with System Owner and System Administrator and Second Level Support Personnel
  - Coordination and Planning of Post Assessment Meeting
  - Review Scan Data and Draft POA&Ms
  - Conduct Post Assessment Meeting

Security Posture Assessments Process

- **IRAT conducts the following activities as part of the Security Posture Assessment Process**
  - Develop System Test Plan
    - Is based on the SCD and identifies assets that will be tested, Operating Systems, Databases, Web Sites, and exposure level of each asset
    - Identifies Test tools that will be used to conduct testing
    - Access to system assets is required to conduct security testing

Security Posture Assessments Process

- Perform System Testing / Data Gathering
  - Conduct In-Brief
  - Perform System Walk Through to Validate System Architecture, Assets, and Interfaces
  - Conduct Interviews of System Specialists and System Management Personnel and Collect Artifacts
  - Review Open POA&Ms
  - Conduct On-Site Testing Activities
  - Site Exit and Follow-Ups

Security Posture Assessments Process

– Data Analysis and Upload Test Data to Repository

- Compliance with ATO Security Requirements
  - Determine if each security control is implemented, or not implemented, in the fielded system configuration.
- Analysis of SSP
  - Determine if the security controls identified in the SSP are implemented in the fielded system configuration. Differences between security controls identified in the SSP and the fielded system are identified and documented.
- Analysis of Test Data
  - Compliance with approved secure configuration baseline standards
  - System Hardening (e.g., use of unnecessary ports and services),
  - Patch Management, and
  - Implementation of Anti-Virus
  - Artifact review for validation.

Security Posture Assessments Process

- Develop Security Assessment Report (SAR)
- The IRAT system assessors develop the SAR and SAR App A, which are developed in accordance with the milestones in the Master Schedule. The assessment methodology is in accordance with:
  a. NIST SP 800-37 Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems and
  b. NIST SP 800-53A, Guide for Assessing the Security Controls in Federal Information Systems.
- Draft POA&Ms are developed when the implemented system security configuration is noncompliant with security control requirements.
- The draft POA&M, SAR, and SAR Appendix A are then forwarded to the system's ISSO to continue the authorization process.

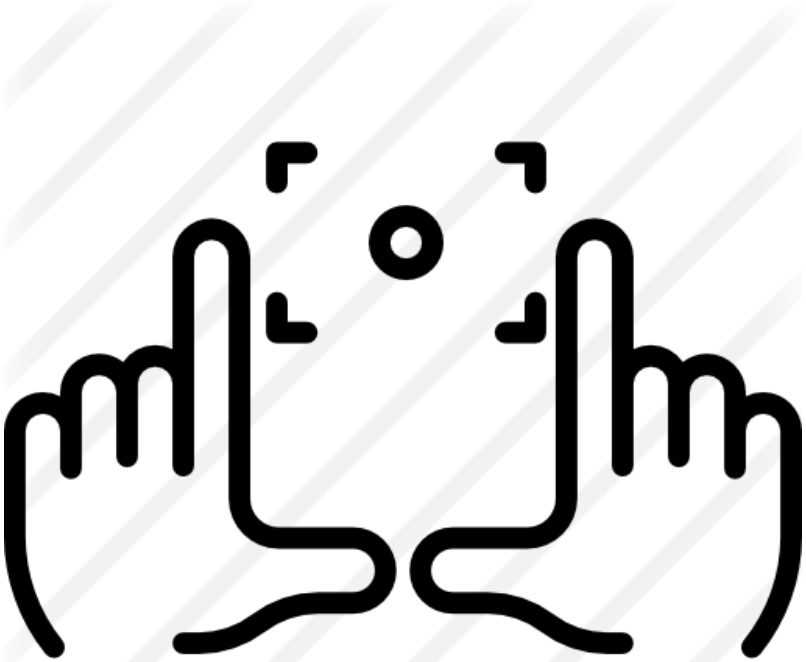
Requirements Fulfilled by Penetration Testing

- From FY2020 ATO Baseline: Tailored ATO Requirements (NIST SP 800-53R4):
  - CA-2 / **System Owners** must ensure that security requirements compliance and vulnerability testing are performed annually as defined in the ATO Information System/Security Continuous Monitoring (ISCM) Plan and authorization master schedule. **Assessment testing must include penetration testing in accordance with the DOT Compendium.**
  - CA-8 / **System Owners** must ensure that the ATO Information Systems Security (ISS) Program **performs penetration testing annually**, on system threat entry points assets that pose a potential threat. The ATO ISS Program must use an independent testing entity.

How do we help fulfill testing requirements?

- Experienced testers with skillsets stretching across government and commercial sectors
- Rules of Engagement (RoE) tailored for the NAS environment
- Threat emulation based on real-world threats and attack vectors
- Test events designed specifically to address NIST 800-53 requirements
- Identify or establish threat information sharing with other agencies and commercial sector
- Customize Tactics/Tools, Techniques, & Procedures (TTPs) for NAS system deployments

FAA's Scope of Testing



- Utilize lab and system environments
- Flexibility in scheduling around system owner needs
- Current and legacy technology
- Not limited to IP testing

NAS Cyber Engineering Facility (NCEF)

- The NCEF is a Technical Operations resource supporting the enterprise information security engineering needs for all Air Traffic Organization (ATO) NAS and non-NAS systems.
- It is a tactical, NAS Systems Engineering facility that supports ATO cybersecurity, in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond, Recover).

- Functional Areas of Responsibility:
  - ❑ Enterprise Security Management
  - ❑ Enterprise Solutions Development
  - ❑ Incident Response Support
  - ❑ Boundary Protection
  - ❑ Agile Workpile

NAS Cyber Engineering Facility (NCEF)

- **Enterprise Security Management:** The NCEF houses facilities, resources and tools to support strategic ATO Enterprise Security Management. These capabilities provide the ATO with insight into enterprise wide security issues to facilitate a broad range of security governance and risk management functions.
  - **Services**: Data collection and aggregation, metrics and analytics, health and integrity monitoring.
  - **Tools**: Enterprise risk assessment tools, data repositories, database maintenance tools, security and metrics tools, equipment HW and SW monitoring.
- **Enterprise Solutions Development:** The NCEF provides foundational support for the development of security solutions having enterprise value and impact. The NCEF facility also provides an area for experimentation and investigation in information security concepts and techniques.
  - **Services:** Security solutions R&D, security solutions testing and deployment, technical support and assistance.
  - **Tools:** Vulnerability management tools, research and development tools, test results repositories, testbeds and scenarios, technical support/training tools.

NAS Cyber Engineering Facility (NCEF)

- **Incident Response Support:** The NCEF is uniquely positioned to support a range of ATO incident response elements. The NCEF provides situational awareness through the implementation of various informational feeds, and provides the tools and facilities to support analysis and tactical response.
  - **Services**: Situational awareness, tactical field support.
  - **Tools**: NAS awareness, NAS system support, ACG support, NOCC/NCO support.

- **Boundary Protection:** The NCEF supports the development, implementation, and operation of boundary protection measures.
  - **Services**: Program management, develop, test and implement solutions, operational maintenance and support.
  - **Tools**: VMAG, future OSE/MS border protection, monitoring, maintenance and administration.

- **Agile Workpile:** The NCEF technology and resources support a multitude of ATO ad hoc and quick response information system security (ISS) needs.
  - **Services**: Ad Hoc security support, quick response.
  - **Tools**: All NCEF and ACG tools, assets and capabilities.

NAS Cyber Engineering Facility (NCEF)

NCEF Processes and Timelines

- The NCEF team is in the process of implementing development, test, and production VMware environments to support ACG tools such as NORA, ATOM, IRIS, and Service Now.
- Conducting ongoing analysis and testing on edge devices such as Data Diodes, Network Taps, and KVMs.
- Working with the Cyber Engineering team on the development and implementation of Vendor Management Access Gateway (VMAG). The timeline to begin pilot testing is set for January, 2021.
- Implementing VMware environments to support IRAT testing of data analytics, remote scanning solutions utilizing FNTB, and a new Cyber Range platform that will be utilized for cyber warfare testing.
- Conduct security posture scans on new NAS and non-NAS systems to help identify vulnerabilities and risks ahead of IRAT scans / Authorization.
- Provide ongoing ISSO support: (i.e.) POAM remediation, enhanced data collection.

NAS Cyber Engineering Facility (NCEF)

Cyber Hygiene: The NCEF utilizes a cyber hygiene routine to reduce the system's vulnerabilities and threats, and improve security. This includes:

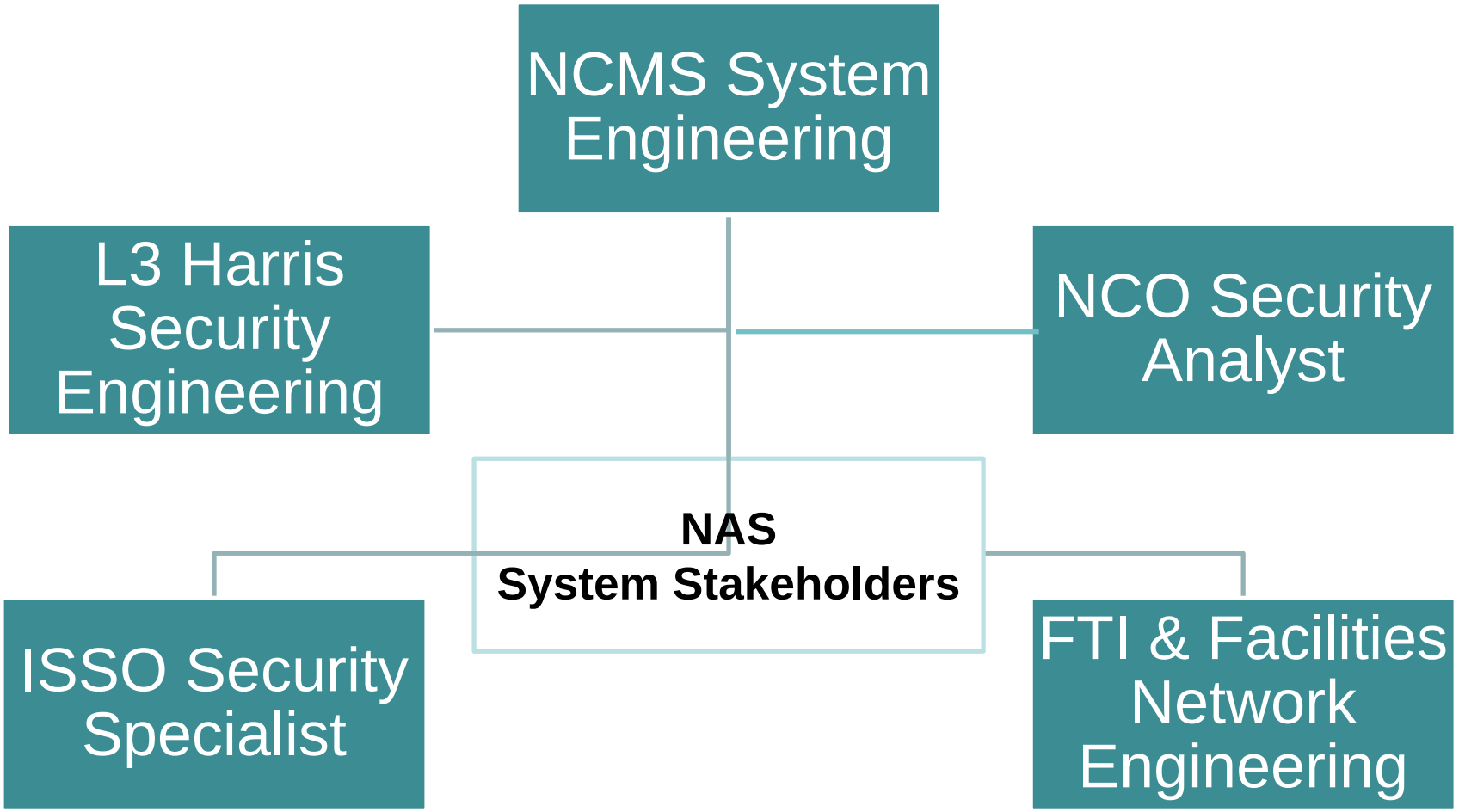
- Documenting all current equipment and programs (hardware, software, and applications);
- Documenting all standard operating procedures;
- Maintaining all Operating System (OS), application software, web browsers, and firmware with latest security patches;
- Enforcing strong password rules / password policy;
- Ensuring that all anti-virus (AV) is installed and configured;
- Ensuring that all computer networks are physically segmented with secure routers and active firewalls between segments;
- Enforcing user request forms to limit user access;
- Enforcing service request forms to manage system change requests;
- Enforcing a process for adding new edge border devices to approved device lists;
- Utilizing Backups to protect from data loss.

NAS Cyber Management System

- NCMS employs multiple remote Connectors as event collection points, enterprise wide, for systems across the NAS.
- Working with the program stakeholders and system engineers we on-board NAS IP based assets to stream syslog data to the Tech Center in Atlantic City, NJ for storage and archiving and to the NAS Cyber Operations center in Warrenton, VA.
- The NCO group provides near-real-time event monitoring, analysis, and coordinated response to all NAS cyber security incidents.
- As an added benefit, NCMS provides system owners some inherited compliance of SP800-53 controls using an enterprise level solution.

- **Event Auditing – NCO/NCMS**
- **Event Monitoring – NCO**
- **Cyber Response - NCO**
- **Reporting – NCO/NCMS**
- **Syslog Storage – NCMS**
- **Event Archiving – NCMS**

NCMS On-Boarding Team



NCMS Onboarding Process
PHASE I – Technical Integration

- **Technical Integration Meeting**

  System owners learn about NCMS and the NCO functions. What to expect and how to connect their assets. We learn about their systems and how they do business in the NAS.

- **Asset Information List**

  We ask the system owners to provide a comprehensive list of system assets and we use that to develop parsing and mapping files.

- **Develop a Test Schedule**

  We then identify and prioritize a timeline for testing each type of asset used in production.

NCMS Onboarding Process
Phase II - Testing

- **System FNTB Connectivity**

  Establish a viable test connection using the FAA National Test Bed (FNTB) facilities

- **NCMS Validation**

  Identify and correct connectivity issues, with the help of FTI facility engineers. Identify and correct critical information needed to onboard a system; assets, site, hostnames and IP addresses

- **Parsing & Mapping**

  Identify and correct event log format and field parsing issues with the help of NCO analysts and L3 Harris engineers

- **Final NCO Validation**

  NCO analysts make the final determination that testing is complete

NCMS Onboarding Process
Phase III - Cutover

- **System Cutover Schedule**

  Identify system deployment, tech refresh, and adaptation schedules to bring NAS assets online with NCMS

- **Asset Information List is Complete**

  Do a final review of all operational assets, sites and any backend devices.

- **Parsing and Mapping Installed**

  Duplicate the parsing and mapping strategies for operational connectors that were developed during the Test Phase.

- **Final Validation**

  Events received match the asset information provided by the system owners.

- **NCO Event Baseline and Characterizations**

  The NCO develops a baseline characterization of the operational system over time.