

2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | “Cyber Hygiene”

Operational NAS Assessment Team

Date: October 20, 2020



**Federal Aviation
Administration**



Integration Outreach and Planning (IOP)

- **Mission: To protect the “Operational NAS” from internal and external vulnerabilities and confirm security control compliance at airports and control centers**
- **Role: Conducts operational security assessments in an Air Traffic “live” environment**



Functional Area of Responsibility

Evaluate 33 NIST Controls within the below hierarchal control families in the “live” NAS.

- Access Controls (AC)
- Audit and Accountability (AU)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Responses (IR)
- Maintenance (MA)
- System and Information Integrity (SI)



Phased Approach Plan

- Fully brief all field Stakeholders/Union well in advance
- Brief Cybersecurity Risk Management Framework 101
- Observe ORM
- Perform auditing of Files and Artifacts collected in the Operational Facility
- Time at facility is 1 to 2 days
- Gather data and lessons learned
- Create Security Assessment Report (SAR) within 90 days of assessment
- Create POA&Ms
- Create an Executive Report w/Field findings
- Perform Field Remediation with Field facility



Roles and Responsibilities

- Information System Owners - Create, authenticate, disseminate, lab procedures (Test Plan) and participate in SAR findings/final reports
- ATSSs for systems under evaluation - Perform system key strokes for the configuration logs and configuration files, with SLE will support, if necessary
- AJW-B4 assist in creating the IRMC/IRMP prior to arrival
- IRAT perform interviews, creates SAR within 90 days



Roles and Responsibilities

- Union engagement; both PASS and NATCA briefed/National and Locally, national agreements are in effect
- ACG collaborates findings with key stakeholders and creates an Executive Report for signature. Contacts field for “Remediation” when they are the OPR of findings



PHASE II

- With an established Performance Audit and Data gathering and lessons learned from Phase I...Perform Scan Evaluation
- Phase II encompasses all activities in Phase I along with scanning of support/test assets in the field (where appropriate)

