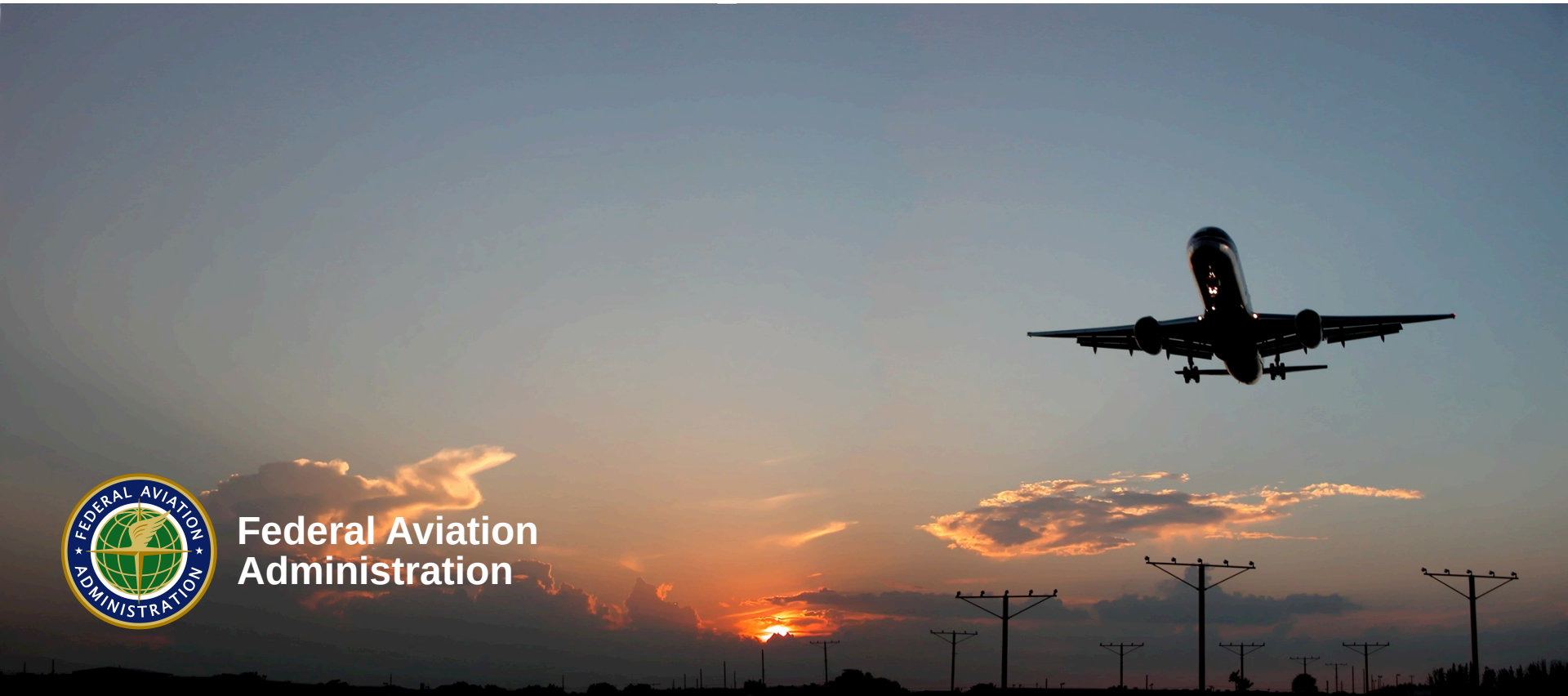
2020 FAA Cybersecurity Awareness Symposium

Securing the Aviation Ecosystem | "Cyber Hygiene"

NAS Edge Device Evaluation Process

Date: October 20, 2020



Background

- **ATO Orders do not currently provide guidance for certain types of devices that cross the NAS/Non-NAS boundary**
  - Peripheral Sharing Systems (aka KVM switches)
  - Network Test Access Points (aka TAPs)
  - Data Diodes
- **June 2019 – Memo issued by ACG provides guidance to ISOs to coordinate with ACG for a technical assessment, evaluation and approval of NAS Edge Devices**

Discovery

- **Information System Owner (ISO)**
  - Identify proposed devices and location/use within system architecture and notifies ISSO
  - Coordinate with vendor to obtain information about the device
  - Brief proposed architecture, device locations and use to ACG

Discovery

- **Information System Security Officer (ISSO)**
  - Verifies if device is on the ACG approved device list. If device is on approved device list, advise ISO to proceed
  - If the device is new, request ISO to coordinate with vendor to provide vendor device guides or any other information about the device and provide a test unit if available
  - The ACG Approved Device List is on the ACG KSN

Technical Analysis

- **Cyber Engineering Team**
  - Analyze device guides and other information about the device
  - Meet with ISO and ISSO, if needed, to get additional information
  - Evaluate device architecture and configuration to determine if there are any security concerns

Technical Analysis

- **Cyber Engineering Team**
  - Develop requirements for the configuration, management, testing and hardening of each new device and recommend specific test cases be run against the device
  - Provide new device requirements to the Cyber Testing Team

Pre-Testing

- **Pre-Testing - Cyber Engineering (CE)**
- **and Cyber Testing (CT) teams**
- **“Collaborative effort”**

  – CE team develops ATO ACG requirements and hands off to the CT team to test against the device

Pre-Testing

- **NAS System specific requirements to CT such as:**
  - "The device shall have a packet loss ratio of less than 0.001"
- **CT team performs an analysis and determines if physical device testing shall be performed**
  - The new device shall be provided to the CT team by the vendor and/or ISO, with coordination through ISSO

Analysis Evaluation

- **Analysis Evaluation (CT team)**
  - Develops evaluation methodology: test plan and procedures
  - Acquire device capability Matrix from the vendor
  - Obtain third party, independent testing results, if available:
    - National Information Assurance Partnership (NIAP)
    - Common Criteria (CC) Evaluation Assurance Level (EAL)

Analysis Evaluation

- **Analysis Evaluation (CT team)**
  - Conduct evaluation in accordance to analysis plan, includes NIAP, CC EAL, etc. testing results, reports and certifications
  - Capture evaluation results
  - Provide analysis evaluation results to Cyber Engineering for review

Device Testing

- **NCEF Testing (CT)**
  - Develops test plan and test procedures
  - Obtain devices for testing
  - Obtain commitment from the vendor to provide support during the testing, if applicable

Device Testing

- **NCEF Testing (CT)**
  - Conducts test in accordance to test plan/procedures in the NCEF and/or NAS system lab environment
  - Captures test results in test report
  - Provide the device test results to Cyber Engineering for review

Post-Testing Process

- **Post-Testing (CE Team, CT Team, ACG Managers)**
  - Cyber Engineering team reviews the test or evaluation results
  - Cyber Testing team briefs test results
  - Cyber Engineering develops an equipment recommendation
  - Cyber Engineering Team briefs recommendation to ACG Team Managers

Post-Testing Process

- **Post-Testing (CE Team, CT Team, ACG Managers)**
  - ACG Team Managers make decision on equipment and brief ACG Group Manager
  - Approved equipment added to pre-approved list
  - Cyber Testing Team provides notification to ISSO
  - List of approved equipment is published on KSN site