

# 2020 FAA CYBERSECURITY AWARENESS SYMPOSIUM "CYBER HYGIENE"

## CYBER ENGINEERING (CE)

The National Airspace System (NAS) Cybersecurity Enterprise/Engineering Facility (NCEF) is a Technical Operations (TechOps) resource supporting enterprise cybersecurity engineering needs for all Air Traffic Organization (ATO) NAS and non-NAS systems. One of the capabilities within the NCEF is NAS Edge Device Evaluation. The ATO Cybersecurity Group (ACG) provides guidance to Information System Owners (ISOs) to coordinate with ACG for a technical assessment, evaluation, and approval of NAS Edge Devices. Below are the six process areas.

- 1. Discovery:** The ISO identifies the device, coordination with vendor to obtain information, and briefs architecture to ACG. Information System Security Officer (ISSO) validates if device is on ACG approved list. If the device is new, ISO provides vendor guides or a test unit. The ACG approved list is on the AJW-B4 KSN site.
- 2. Technical Analysis:** The ACG Cyber Engineering (CE) team analyzes the device, evaluates device architecture and configuration to determine if there are any security concerns, develops requirements for configuration, management, testing and hardening along with specific tests cases to be run against the device. Requirements are provided to the ACG Cyber Testing (CT) team. **Below are: KVM, TAP, and Data Diode**



The NCEF is a tactical NAS Systems Engineering facility that supports ACG in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Identify, Protect, Detect, Respond, and Recover).

- 3. Pre-Testing:** The ACG CE team develops ACG requirements and hands off to the ACG CT team to test against the device. Specific ISO requirements are incorporated into the test plan. Analysis is performed to determine if device testing needs to be performed.
- 4. Analysis Evaluation:** The ACG CT team develops evaluation methodology for the test plan and procedures, and then acquires vendor information, and obtains independent testing results. Evaluation is conducted in accordance to the analysis plan. Evaluation results are captured and are provided to the ACG CE team for review.
- 5. Device Testing:** The ACG CT team develops test plans and procedures in parallel with obtaining a device and support from the vendor. Testing in the NCEF facility begins and then results are captured and provided to ACG CE team for review.
- 6. Post Testing:** ACG CT team briefs test results to the ACG CE team to develop an equipment recommendation briefing to ACG managers for decision. Approved devices will be added to the pre-approved list on the ACG KSN site. ACG CT team informs the ISSO that the device has been approved. ACG CE team procures equipment through SAVES. Approved NAS Edge Device equipment will be sent to the FAA logistics Center for ordering (future).