2020
FAA CYBERSECURITY AWARENESS SYMPOSIUM
THEME – "CYBER HYGIENE"

CYBER TESTING

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

Requirements Fulfilled by Penetration Testing: FIPS 199 High Systems

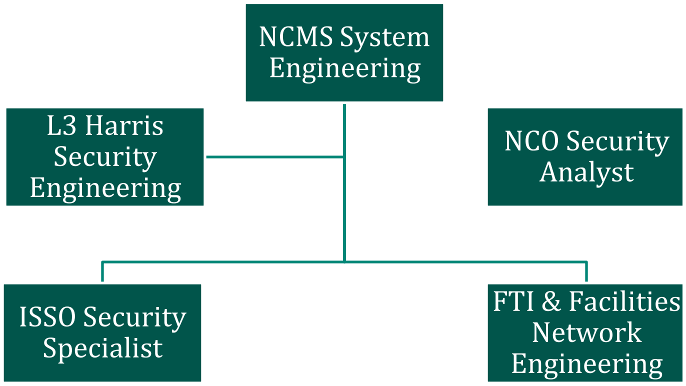
- CA-2 / System Owners must ensure that security requirements compliance and vulnerability testing are performed annually as defined in the ATO Information System/Security Continuous Monitoring (ISCM) Plan and authorization master schedule. Assessment testing must include penetration testing in accordance 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.

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.

NCMS On-Boarding Team



NCMS System Engineering

L3 Harris Security Engineering

NCO Security Analyst

ISSO Security Specialist

FTI & Facilities Network Engineering