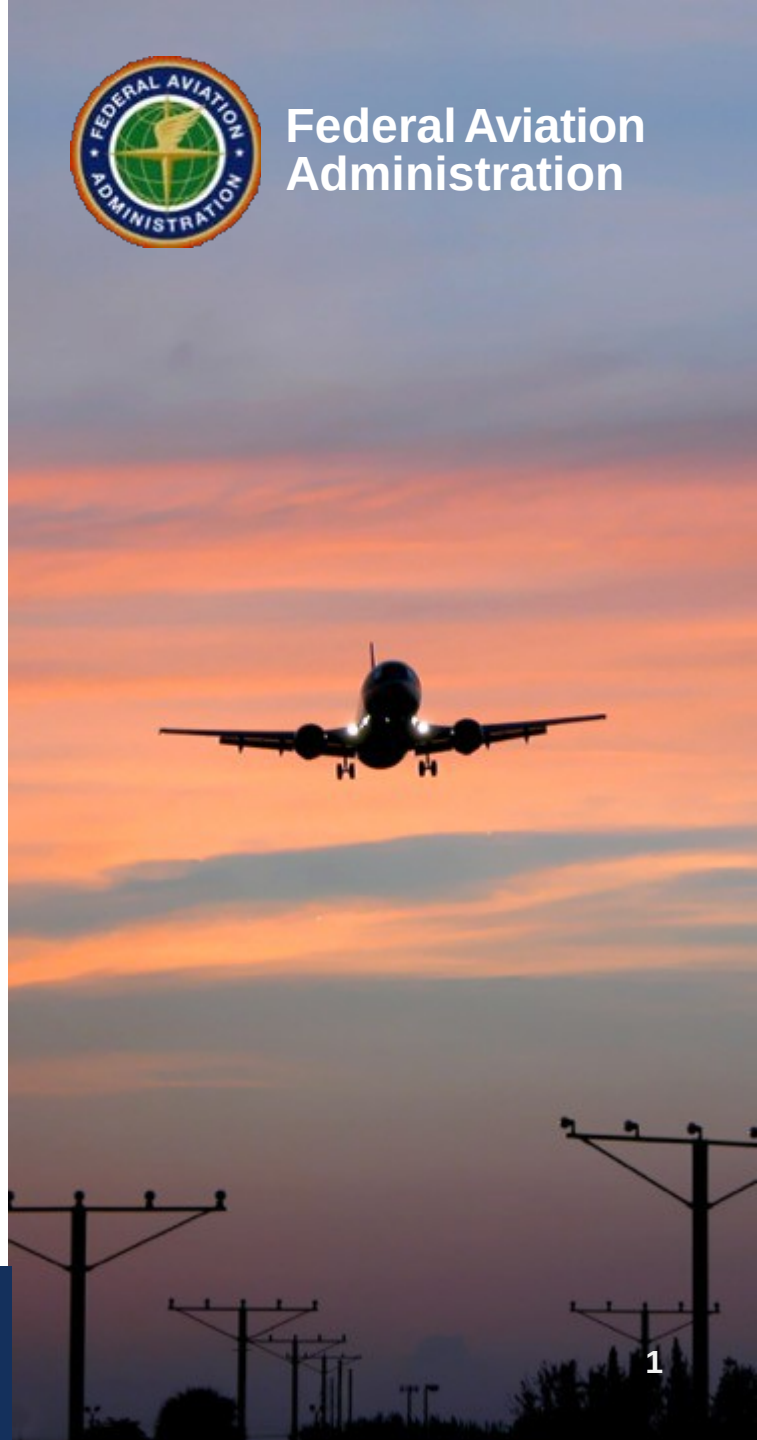
Federal Aviation Administration

FAA Penetration Testing Training & Outreach

Cybersecurity Testing



Version 1.0

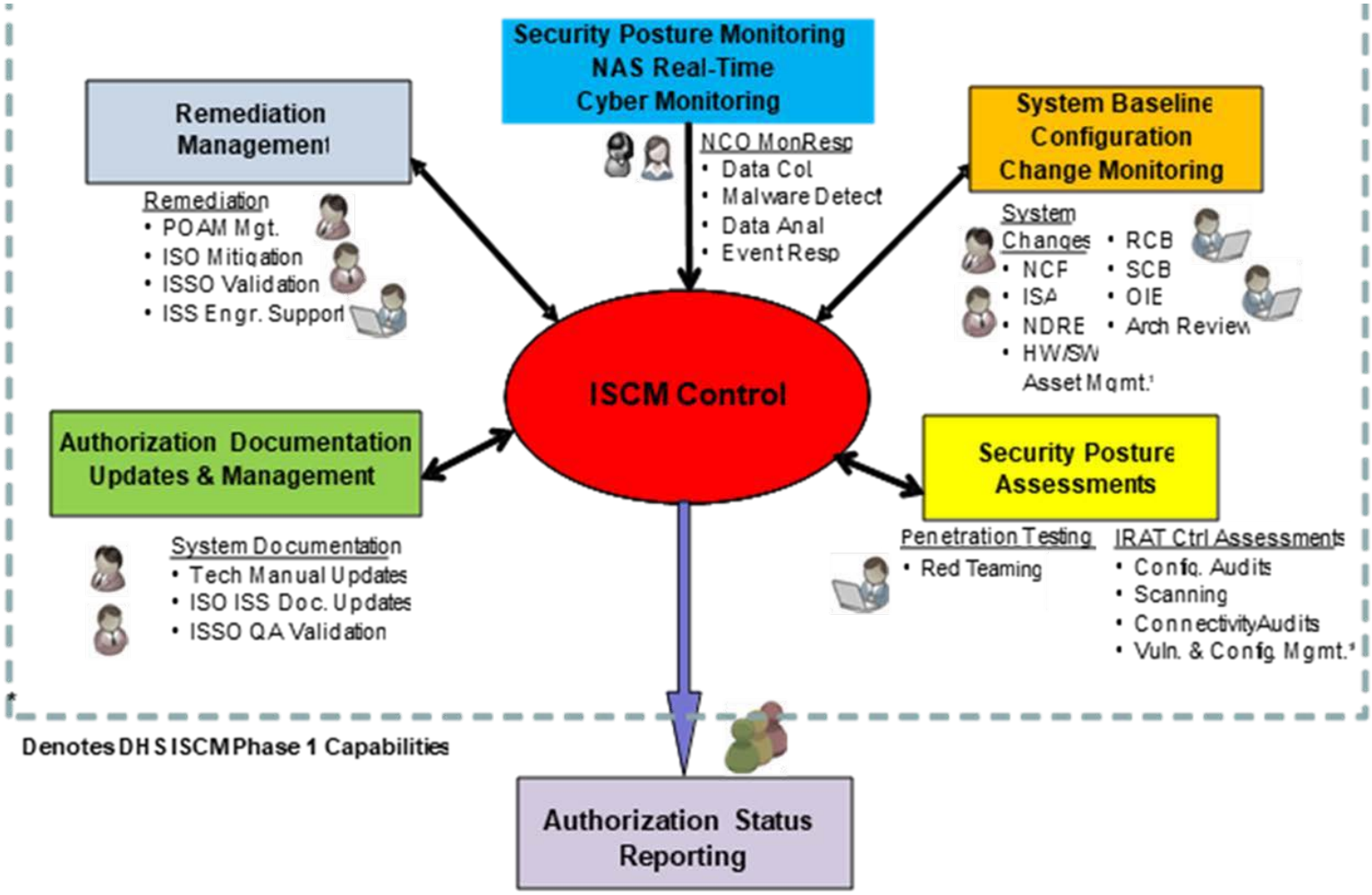
Introduction

- This session is designed to convey:
  - What exactly is penetration testing, why it is needed?
  - What does a ‘normal’ penetration test look like?
  - The general standards and guidelines we meet by performing test events
  - How the FAA’s environment differs from that of a typical enterprise
  - Introducing the penetration testing team
  - Milestones and plan moving forward

Agenda

- Org Chart
- Penetration Testing Team
- Where Penetration Testing Fits
- Current Status
- Requirements Fulfilled by Penetration Testing
- Definitions from NIST
- FAA's Environment
- How do we help fulfill testing requirements?
- FAA's Scope of Testing
- Tools & Techniques
- Testing Cycle
- Planning a Test Event
- Rules of Engagement
- Test Event Pre-Brief
- Test Event Execution
- Recovery, Clean-Up, and Hotwash
- Final Report & Remediation Recommendations
- Testing Accommodations
- Penetration Testing & Broader NAS Testing Approach
- Testing Benefits Recap
- Questions?

Where Penetration Testing Fits



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.

Definition

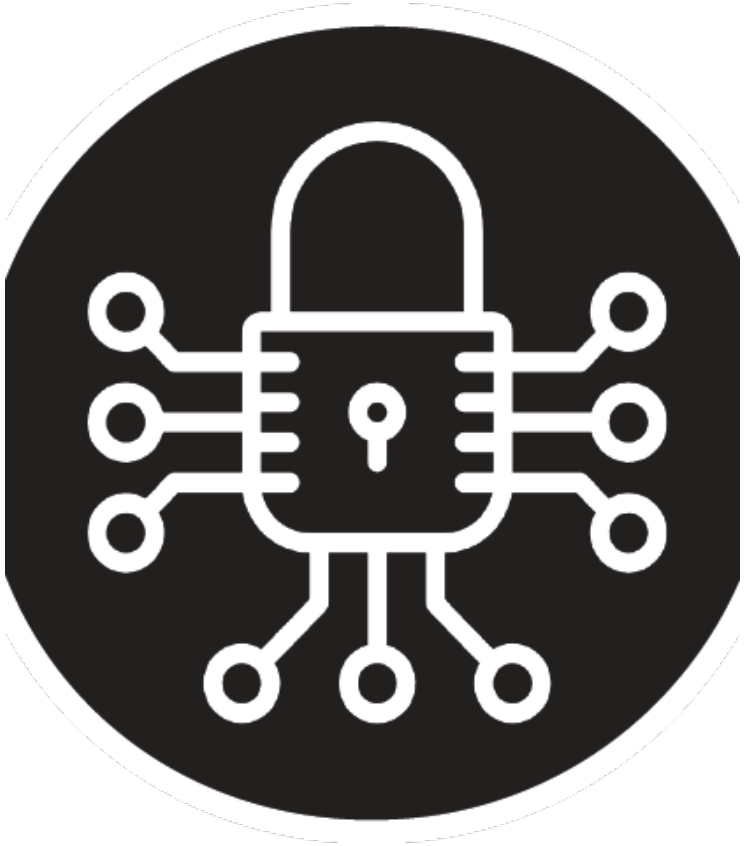
Penetration Testing -

- Penetration testing is an **offensive security exercise** conducted by an organization with the intent to uncover security weaknesses and ultimately help strengthen their defense mechanisms, threat detection capabilities and response times. –Pentest Geek

Red Team Testing -

- “Red team exercises reflect **simulated adversarial attempts** to compromise organizational mission/business functions and provide comprehensive assessment of the security state of information systems and organizations.“ –NIST

FAA's Environment



- FAA Specific Requirements:
  - FAA Mission Statement: "**Our continuing mission is to provide the safest, most efficient aerospace system in the world.**"
  - Air Traffic Control (ATC) operations cannot be interrupted
  - Highly customized and/or proprietary systems and components
  - Complex interconnect of computer systems, networking technologies, air traffic terminals, radars, GPS/ADS-B, weather feeds and other intricate systems
  - System scheduling & availability

How do we help fulfill testing requirements?

- Experienced penetration 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

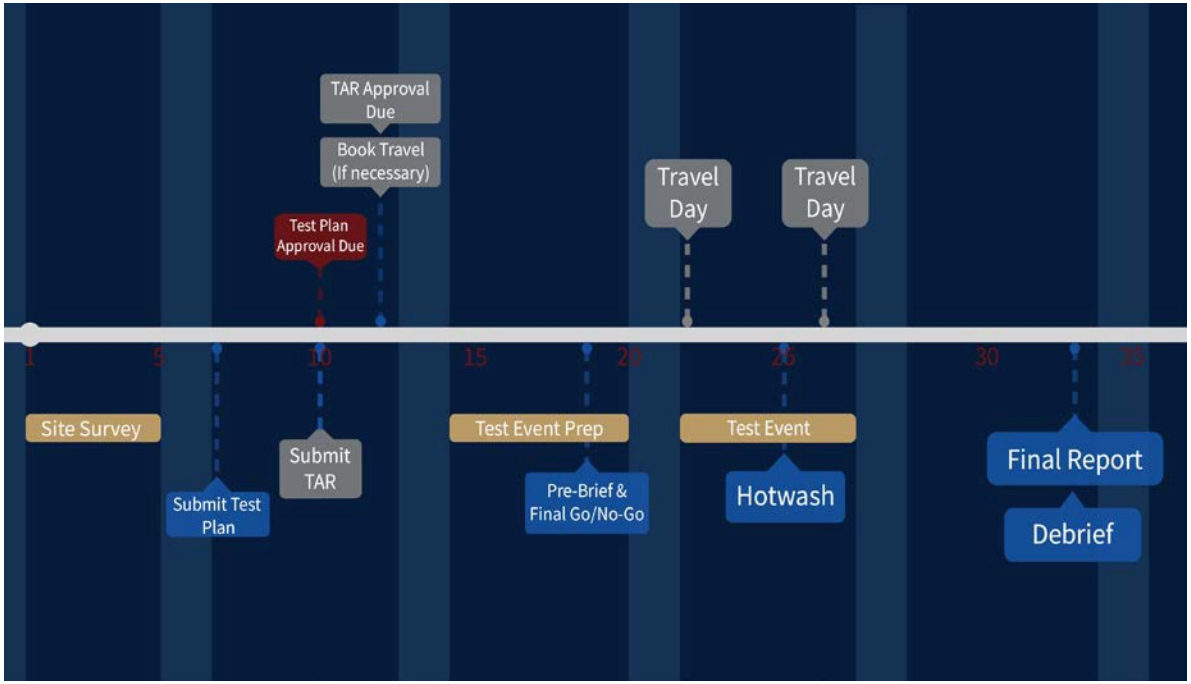
- Utilize lab and/or available test systems
- Tech Center, possibly Log Center, and others
- Flexibility in scheduling around system owner needs
- Ability to test subsystems and/or components if necessary, in lieu of entire system availability
- Legacy technology
- Not limited to IP testing

Tools & Techniques

- Toolkit tailored for each test event
- Emulate external, internal, remote internal, and insider threats
- Implement specialized equipment to allow for efficient use of time Employ virtual environments for increased safety of test equipment (contamination)
- Validate vulnerabilities identified by engineers and technicians
- Utilize threat feeds, tools, and techniques from government/commercial sources

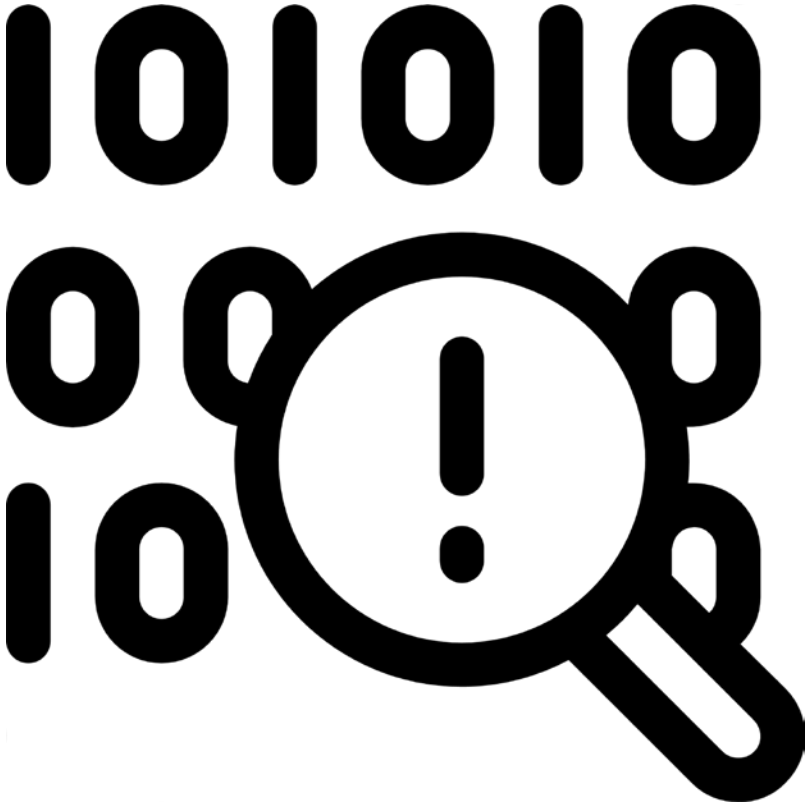
Testing Cycle

- Site Survey
- Test Plan
- Test Event Pre-Brief
- Test Event
- Hotwash
- Final Report
- Debrief



Planning a Test Event

- Identify system(s) to be tested
  - ACG priorities
  - System/String availability and accessibility
- Mission analysis
  - How will we achieve the desired result?
  - What are the Rules of Engagement (RoE) & limitations on the team?
  - How will we know when we've accomplished our goal?
- Conduct site survey
- Research possible attack vectors
- Plan scenarios appropriate for the environment
- Submit test plan and proposed attack vectors for approval by system owners and by FAA Cyber Testing Manager

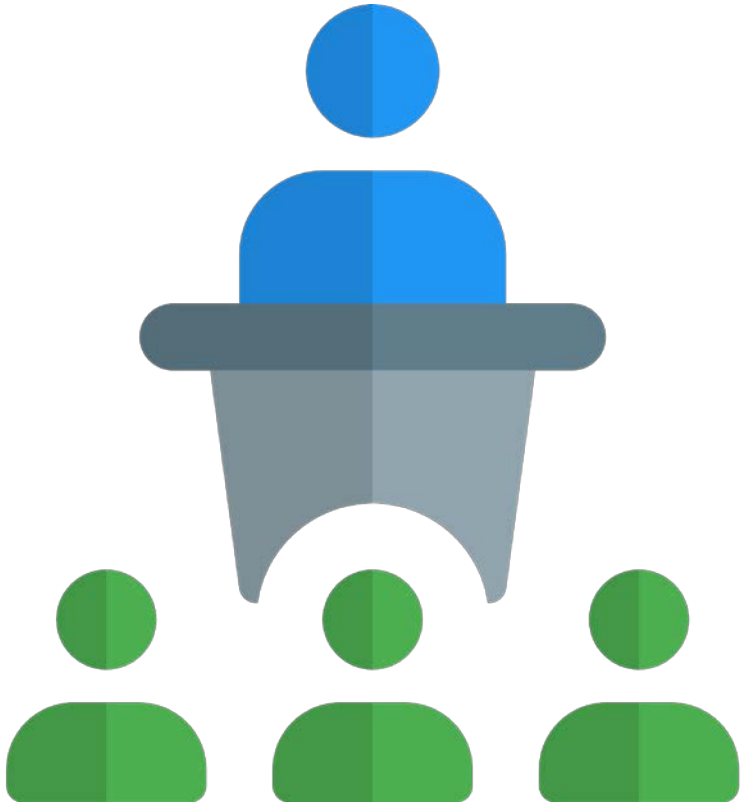


Rules of Engagement

- Testing will adhere to established and agreed upon Rules of Engagement (RoE)
- All testing will be performed on GFE laptops
- Factors for consideration within a tailored RoE include, but are not limited to:
  - Physical destruction of equipment
  - Removal of government equipment
  - Social engineering (e.g. phishing, in-person, phone/SMS, etc.)
  - Connectivity with any additional network (Internet, other FAA networks, VPNs, etc.)
  - Handling of proprietary data (e.g. source code from vendors, FAA sensitive data, etc.)
- The RoE will clearly state the rules and boundaries of the test
- System-specific NDA's as required

Test Event Pre-Brief

- Briefing for key stakeholders
- Review test plan & schedule
- Ensure all questions and concerns are addressed prior to test event
- Allows for last-minute adjustments and accommodations
- Final “ready to proceed” call from ACG management and system owners (Go/No-Go)



Test Event Execution

- Testing occurs as outlined in the approved Test Plan
- Penetration testing team on call 24/7 during the test event (at least one PoC)
- Identified key stakeholders can pause/cancel the testing at any time
- Testers available to give real-time feedback as requested
- Supports approved observers as appropriate
- Suspend testing for approved operational priority
- Realtime investigation of ATC operational impact

Recovery, Clean-Up, and Hotwash

- Full detail of attacks can be recorded as required
  - Ensure clean-up of critical system
  - Later forensic analysis
  - Recreating the exploit
- “Jumping” (re-imaging/re-installing) the system to clean any artifacts is recommended to ensure system integrity
- Hotwash:
  - Informal and informative
  - Provide immediate reinforcement
  - Provide platform to discuss test event and findings
  - Concludes test event

Final Report & Remediation Recommendations

Final report delivered 1 week after end of test event

- Report delivered to Cyber Testing manager and any key stakeholders listed on the test plan
- Stored on secure FAA KSN site

Detailed overview of everything that took place in the test event

- Contains Sensitive Security Information (SSI)
- All attack vectors attempted
- Results of attack vectors
- Screen captures and other "proof" where appropriate

Remediation suggestions are included in the final report

- Recommendations tailored for NAS environment (e.g. IDS vs IPS)

Operational or mission impact analysis

- Real-time and post-test analysis summary
- Recommendations for post-test analysis

Testers available to answer questions about final report or remediation suggestions

- Contact information of testers is included in report, along with all key stakeholders
- Findings should be provided securely, so no vulnerability information is leaked to unauthorized parties

Testing Accommodations Required

Test systems and components

- Systems hardware, software and configuration must be as close as to their production counterparts as possible

Access:

- On-site
- Remote via VPN and/or jump box (if applicable)

When applicable:

- Operators on-station, simulating normal work/operator functions

System Subject Matter Expert (SME) available during test

- To start the event
- To answer questions during the event
- To ensure proper functionality of tested systems

Penetration Testing & Broader NAS Testing Approach

- Strategy Document Contents:
  - Background & Purpose
  - Controls
  - FAA's Operating Environment
  - Penetration Testing Team Structure, Skillsets, and Training
  - Prioritization of Systems to Test
  - Test Event Generic Schedule
  - Testing Methodology (TTPs)
  - Future integration with Code Review in SDLC
  - Mission Impact
  - Findings
  - Policy Implementation Recommendations
  - Threat Intelligence & Information Sharing
  - Vendor Collaboration
  - Training & Outreach
  - Measures of Performance
  - Applicable Appendices

Testing Benefits Recap

- Guided assistance in order to comply with ATO tailored requirements for NIST 800-53 CA-2 and CA-8
- Results that help you determine where to focus time and effort
- Remediation recommendations tailored for the NAS environment
- Penetration testers available to answer questions for your engineers, technicians, and other staff
- Validate vulnerability concerns from system owners & engineers.

Questions?