CYBER TEST AND EVALUATION IN THE US AIR FORCE

Joseph Nichols, PhD
Technical Advisor for Flight Test and Evaluation
Air Force Test Center
Edwards AFB CA
joseph.nichols.13@us.af.mil

Distribution A: Approved for public release; distribution unlimited. 412TW-PA-17133
WHAT IS CYBER TEST AND EVALUATION?
DIACAP Compliance Check

Are you compliant with these controls?

☐ Yes
☑ No

What is the vulnerability level (Severity Category/code)?

☑ CAT I Finding

Process Complete

Risk Management Framework

Are you compliant with these controls?

☐ Yes
☑ No

What is the Risk?

☑ Vulnerability level (includes STIG findings)
☑ Associated Threats
☑ Likelihood of Exploitation
☑ Impact level (CIA)
☑ Compensating Controls and Mitigations

What is the Residual Risk? What is my organization’s risk tolerance? What is my risk tolerance?

☐ Risk Accepted

CERTIFICATION & ACCREDITATION EVOLUTION
CERTIFICATION AND ACCREDITATION VERSUS TEST & EVALUATION

Risk Management Framework

• Compliance with cybersecurity policy (DoDD 8510.01)
• Risk mitigation and acceptance
• Issuance of IATT or ATO

Cyber Test Requirements

• Specification Compliance
• Mission suitability
• Survivability
Airworthiness Requirements

• Compliance with design criteria (MIL-HDBK-516)
• Risk mitigation and acceptance
• Issuance of Type Certificate or MFR

Flight Test Requirements

• Specification Compliance
• Mission suitability
• Survivability
WHAT IS A CYBER SYSTEM?
MILITARY AND INDUSTRIAL SYSTEMS ARE DIFFERENT FROM STANDARD COMPUTER NETWORKS
CYBERSPACE TAXONOMY

- Traditional IT
- Industrial Infrastructure
- Platforms
AF CYBER BOUNDARY FRAMEWORK
WHEEL OF ACCESS
WHAT IS THE CYBER TEST PROCESS?
Risk Assessment

**Likelihood of Attack**

- **O-5**: L-2, L-3, L-4, L-5, L-5
- **O-4**: L-2, L-3, L-4, L-5, L-5
- **O-3**: L-1, L-2, L-3, L-4, L-5
- **O-2**: L-1, L-2, L-3, L-4, L-4
- **O-1**: L-1, L-2, L-3, L-3

**Likelihood of Attack Success**

- **M-1**: M-2, M-3, M-4, M-4, M-5
- **M-2**: M-2, M-3, M-4, M-4, M-5
- **M-3**: M-2, M-3, M-4, M-4, M-5
- **M-4**: M-2, M-3, M-4, M-4, M-5
- **M-5**: M-2, M-3, M-4, M-4, M-5

**Impact of Loss**

- **I-5**: I-5, I-4, I-4, I-5, I-5
- **I-4**: I-3, I-3, I-3, I-4, I-5
- **I-3**: I-2, I-2, I-3, I-4, I-5
- **I-2**: I-1, I-1, I-2, I-3, I-4
- **I-1**: I-1, I-1, I-1, I-2, I-3
- **I-0**: I-1, I-1, I-1, I-1, I-1

**System Severity**

- **S-5**: S-5, S-4, S-3, S-2, S-1
- **S-4**: S-4, S-3, S-3, S-2, S-1
- **S-3**: S-3, S-3, S-3, S-2, S-1
- **S-2**: S-2, S-2, S-2, S-2, S-1
- **S-1**: S-1, S-1, S-1, S-1, S-1

**Mission Criticality**

- **C-5**: C-5, C-4, C-3, C-2, C-1
- **C-4**: C-4, C-3, C-3, C-2, C-1
- **C-3**: C-3, C-3, C-3, C-2, C-1
- **C-2**: C-2, C-2, C-2, C-2, C-1
- **C-1**: C-1, C-1, C-1, C-1, C-1

**Overall Risk Factor Matrix**

- **Likelihood of Loss**
  - **L-5**: L-5, L-4, L-3, L-2, L-1
  - **L-4**: L-4, L-4, L-3, L-2, L-1
  - **L-3**: L-3, L-3, L-3, L-2, L-1
  - **L-2**: L-2, L-2, L-2, L-2, L-1
  - **L-1**: L-1, L-1, L-1, L-1, L-1

- **Impact of Loss**
  - **I-5**: I-5, I-5, I-5, I-5, I-5
  - **I-4**: I-4, I-4, I-4, I-4, I-4
  - **I-3**: I-3, I-3, I-3, I-3, I-3
  - **I-2**: I-2, I-2, I-2, I-2, I-2
  - **I-1**: I-1, I-1, I-1, I-1, I-1

**Within risk tolerance?**

Likelihood= L-1
Risk= Moderate
MISSION THREAD ANALYSIS METHODOLOGY

**METHODOLOGY**

1. Determine Mission Thread
2. Determine Related Attack Surfaces
3. Mission Critical Vulnerabilities
4. Execute Cyber Test Techniques / Procedures
5. Provide Survivability / Mission Impact Assessment

14
WHAT IS THE STATUS OF CYBER TEST & EVALUATION IN THE USAF?
Continuing to execute DT/OT on traditional IT and weapons platforms for developmental systems and legacy platforms

Executing FY16 NDAA 1647 Cyber Assessments

Stand up of Cyber Resiliency Office for Weapon Systems in 2016

Stand up Cyber Test Group/Squadrons in 2017

Beginning development of the Avionics Cyber Range

Growing USAF cyber test manpower
  - AFOTEC sponsoring cooperative/adversarial assessment teams
  - Major government push to hire/retain certified/experienced cyber testers
DOD direction to conduct a cybersecurity evaluation of all major US weapon systems

Testing must be completed by Dec 2019

Combined vulnerability identification phase

Planning combined DT/OT testing

FY16 NDAA SECTION 1647
CYBER RESILIENCY OFFICE FOR WEAPON SYSTEMS (CROWS)
• DoD test facility capable of conducting cyber testing compatible with the unique features of aircraft avionics and airborne munitions

• Center of Excellence for avionics cyber T&E and developer of cyber test techniques and test tools

• Connected with the NCR and other aircraft and weapons cyber test facilities

AVIONICS CYBER TEST INFRASTRUCTURE
AFOTEC has three cyber missions for DoD and Air Force

- Primary is testing systems in a realistic operational environment
  - Mission assurance and resiliency of systems are test objectives
- Providing cyber mission assessments of PACOM, NORTHCOM/NORAD and as executive agent for Air Force for DOT&E
- Authorizing official for operations test infrastructure

- Teaming with AFTC to provide support for vulnerability analysis, “blue books”, and integrated cyber testing
- Working operational cyber range requirements through AFTC
- Increasing NSA certified Adversary Assessment Team capacity with MOUs with Kansas ANG, Air Warfare Center, and New Mexico ANG
- Total force initiatives—with both AFTC and ANG Readiness Center
Cyber T&E expertise for aircraft and weapons requires a merge of traditional avionics test expertise and computer network penetration expertise.

- Sending avionics test engineers to cyber training
- Developing DOD cyber training courses
- Standing up new test organization dedicated to all aspects of cyber test and evaluation – networks, aircraft, weapons