MARINE CORPS TACTICAL SYSTEMS SUPPORT ACTIVITY

Technical Excellence...Tactical Value

Adversarial Cyber Developmental Test & Evaluation

Major Paul Keener

(Cyber DT&E Lead)

Major Scott Fortner

(SoST Event Director)

Topics

- Background
- Levels of Cyber Testing
- DT&E Requirement
- Value of Adversarial Cyber DT&E
- MCTSSA Cyber Testing
- System of Systems Adversarial Cyber Testing at MCTSSA (A Use Case)
- Cyber Testing Approach
- Major Findings
- Mission Impacts

Background

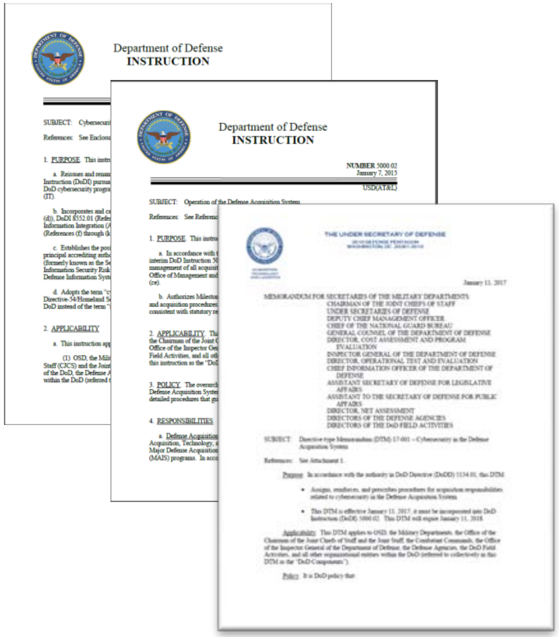
- Historically, programmatic cybersecurity actions have been centered on IA scans (IV&V process)
  - IV&V has significant limitations
- No consistent application of host protection software across systems
  - Functionality is given priority over security
- Penetration testing has predominantly been an OT and operational activity and does not involve all programs/systems

Levels of Cyber Testing

- IV&V
  - Non-destructive evaluation of a single system at a time
  - Common software and operating systems only
  - Focuses on design and functional requirements for individual systems
  - Verify STIGs, policies, and patch compliance
- DT&E (Developmental Test and Evaluation) Adversarial Cyber Assessment
  - Destructive and non-destructive exploitation
  - Single system or system of systems in Mission Context
  - Assesses custom software along with operating systems and hardware
  - Focuses on exploiting vulnerabilities
- OT&E Adversarial Cyber Assessment
  - Non-destructive exploitation
  - System of systems in mission context
  - Conducted in an operational environment with certified red teams
  - Applies social engineering
  - Focuses on identifying vulnerabilities

DT&E Requirement

- **<u>DoDI 8500.01, *Cybersecurity*, March 14, 2014</u>**; establishes that cybersecurity must be fully integrated into the system lifecycle.
- **<u>DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015</u>**; includes regulatory cybersecurity requirements for SE and DT&E; establishes that cybersecurity RMF steps and activities should be initiated as early as possible and fully integrated into the DoD acquisition process.
- **<u>DTM 17-001, *Cybersecurity in the Defense Acquisition System*, January 11, 2017</u>**; directs Adversarial Cybersecurity DT&E to "*Conduct a cybersecurity DT&E event using realistic threat exploitation techniques in representative operating environments and scenarios to exercise critical missions within a cyber-contested environment to identify any vulnerabilities.*"



Department of Defense
INSTRUCTION

SUBJECT: Cybersecuri

References: See Enclosu

1. PURPOSE. This instru

a. Reissues and renam Instruction (DoDI) pursua DoD cybersecurity progra (IT).

b. Incorporates and ca (d)), DoDI 8552.01 (Refer Information Integration (A (References (f) through (k

c. Establishes the posi principal accrediting autho (formerly known as the Se Information Security Risk Defense Information Syste

d. Adopts the term "cy Directive-54/Homeland Se DoD instead of the term "i

2. APPLICABILITY

a. This instruction app

(1) OSD, the Milit Staff (CJCS) and the Joint of the DoD, the Defense A within the DoD (referred t

Department of Defense
INSTRUCTION

NUMBER 5000.02
January 7, 2015

USD(AT&L)

SUBJECT: Operation of the Defense Acquisition System

References: See Referenc

1. PURPOSE. This instru

a. In accordance with t interim DoD Instruction 50 management of all acquisit Office of Management and (ce).

b. Authorizes Mileston and acquisition procedures consistent with statutory re

2. APPLICABILITY. Thi the Chairman of the Joint C Office of the Inspector Gen Field Activities, and all oth this instruction as the "DoD

3. POLICY. The overarch Defense Acquisition Syster detailed procedures that gu

4. RESPONSIBILITIES

a. Defense Acquisition Acquisition, Technology, a Major Defense Acquisition (MAIS) programs. In acco

THE UNDER SECRETARY OF DEFENSE
3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

January 11, 2017

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
CHIEF OF THE NATIONAL GUARD BUREAU
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, COST ASSESSMENT AND PROGRAM EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
CHIEF INFORMATION OFFICER OF THE DEPARTMENT OF DEFENSE
ASSISTANT SECRETARY OF DEFENSE FOR LEGISLATIVE AFFAIRS
ASSISTANT TO THE SECRETARY OF DEFENSE FOR PUBLIC AFFAIRS
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-type Memorandum (DTM) 17-001 – Cybersecurity in the Defense Acquisition System

References: See Attachment 1.

Purpose. In accordance with the authority in DoD Directive (DoDD) 5134.01, this DTM:

- Assigns, reinforces, and prescribes procedures for acquisition responsibilities related to cybersecurity in the Defense Acquisition System.
- This DTM is effective January 11, 2017; it must be incorporated into DoD Instruction (DoDI) 5000.02. This DTM will expire January 11, 2018.

Applicability. This DTM applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this DTM as the "DoD Components").

Policy. It is DoD policy that:

Value of Adversarial Cyber DT&E

- Adversarial cyber DT&E provides destructive and non-destructive penetration testing prior to OT and system fielding
  - Adversarial cyber DT&E can be tailored to the systems under test (SUT) to accommodate assessment of custom software and hardware, as well as evaluation through layers of defense.
  - Reduced risk to the program and the operational commanders
- The developmental test environment is not restricted to simply identifying vulnerabilities
  - Allows for full exploitation of vulnerabilities
  - Highlights true impact to operational mission environment
- Adversarial cyber DT&E provides program decision makers critical information for risk management and vulnerability mitigation

MCTSSA Adversarial Cyber Testing

- MCTSSA conducts DT for USMC C4 programs of record
  - Adversarial cyber testing was added to existing DT events beginning in 2014
- MCTSSA test environments are configurable, scalable, and operationally relevant
  - Operationally relevant environments require a System of Systems approach
- Mission funded - no cost to USMC programs of record (PORs)
- Focus is on the equipment, not the operators
  - Addresses areas that PORs can control

MCTSSA MISSION
MCTSSA provides test and evaluation, engineering, and operating forces technical support for USMC and Joint Service command, control, computer, communications (C4) systems throughout all acquisition life-cycle phases

System of Systems Adversarial Cyber Testing at MCTSSA

(A Use Case)

- USMC initiative to evaluate changes to the Marine Corps Enterprise Network (MCEN) prior to implementation (both garrison and tactical)
- In 4th quarter FY16, we conducted a System of Systems (SoS) test to evaluate enterprise performance for USMC tactical network
  - Fires and common operational picture (COP) missions
- This was the initial SoS adversarial cyber event
  - Previous events were individual system level

Cyber Test Approach

- Constructed an Adversarial Cyber Framework
  - Methodical and repeatable approach
  - Emulated a near sider threat
  - Used common tools
  - Cyber team capable of presenting an advanced (nation-state) threat
  - Scored vulnerabilities using Common Vulnerability Scoring System (CVSS) 3.0
- Focus on impacting the tactical missions
  - Via identification and exploitation of network and system vulnerabilities
  - The goal was to Deny, Degrade, and/or Corrupt mission threads
- Cyber attack team had knowledge of the systems under test and network architecture
  - Facilitated shorter test execution timeframe

Major Findings

- New vulnerabilities were identified on systems with current ATOs, including zero-day vulnerabilities
  - This shows that ATO risk is underestimated
- Custom software cyber hygiene issues (passwords, usernames, # of login attempts) controls not enforced or implemented
- Implementations of HBSS are inconsistent across various programs

Mission Impacts

- Fire Missions
  - Significant delay in fire mission processing (>10 min) – *Degrade*
  - Delays were repeatable and led to complete denial of service – *Deny*
  - Ability to crash/shutdown system – *Deny*
- Common Operational Picture
  - Track injection and blocking – *Corrupt*
  - Communication interruption – *Deny and Degrade*
- Network
  - Ability to take control of local domain – *Corrupt*

Questions?