



Joint Task Force National Capital Region Medical **INSTRUCTION**

NUMBER 8430.01

NOV 15 2011

J-6

SUBJECT: Commercial Off-the-Shelf (COTS) Software Approval Standard Operating Procedure

References: (a) JTF CAPMED-D 5106.01, "Information Assurance Advisory Group (IAAG) Charter," May 10, 2010
(b) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
(c) DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003

1. PURPOSE. This Instruction, in accordance with the authority in Reference (a):

a. Establishes policies and guidelines necessary to execute the security testing procedures for COTS software products used throughout the Joint Task Force National Capital Region Medical (JTF CapMed) to ensure compliance of the security requirements established in Reference (b).

b. Specifically defines the security testing approach, objectives, and procedures utilized to test COTS software products, and serves as a technical specification guide for the proper execution of software testing according to the established requirements.

2. APPLICABILITY. This Instruction applies to JTF CapMed and all Joint Medical Treatment Facilities and Centers in the National Capital Region (i.e., Fort Belvoir Community Hospital, Walter Reed National Military Medical Center, and the Joint Pathology Center).

3. POLICY. It is JTF CapMed policy that COTS software products shall undergo security testing to determine compliance with Reference (c) and security requirements. The candidate software product must meet the criteria documented within the JTF CapMed Software Test Request Worksheet and JTF CapMed Software Evaluation Checklist.

4. RESPONSIBILITIES. See Enclosure 1

NOV 15 2011

5. PROCEDURES. See Enclosure 2

6. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Internet from the JTF CapMed Web Site at: www.capmed.mil.

7. EFFECTIVE DATE. This Instruction is effective immediately.



SCOTT WARDELL
Executive Director for Administrative Operations
By direction of the Commander

Enclosures:

1. Responsibilities
2. Procedures

NOV 15 2011

ENCLOSURE 1

RESPONSIBILITIES

1. JTF CAPMED LEAD ENGINEER. The JTF CapMed Lead Engineer shall:
 - a. Review the JTF CapMed Software Test Request Worksheet from the sponsor.
 - b. Accept the candidate software for inclusion in the JTF CapMed Software Testing process.
 - c. Validate that the results of each test step were correctly executed.
 - d. Verify all documents are properly completed.
 - e. Approve all modifications of, or deviations from, the documented test procedures.
 - f. In the event of an equipment malfunction, software problem, or any other discrepancy, determine, in coordination with the software sponsor, whether the test should proceed or halt until the problem is resolved.
 - g. Ensure the JTF CapMed testing methodologies are properly executed.

2. JTF CAPMED TEST ENGINEER. The JTF CapMed Test Engineer is provided the software and a copy of the approved JTF CapMed Software Test Request Worksheet by the Lead Engineer. The Test Engineer must be readily available during scheduled test periods and shall be responsible for, but not limited to:
 - a. Setting up clean Federal Desktop Core Configuration (FDCC) image(s) for testing.
 - b. Ensuring all raw data test results generated during testing are properly marked with Software Name/Version#/Engineer initials (e.g., QMatics_v1.2_HBH). All data is stored in the JTF CapMed Workspace within the Space and Naval Warfare Systems SharePoint database.
 - c. Ensuring all sensitive material generated during testing is collected, properly marked, and safeguarded as applicable.
 - d. Completing the JTF CapMed Software Risk Assessment Report and submitting to the Lead Engineer via encrypted email.

3. PROJECT SOFTWARE SPONSOR. The software sponsor is responsible for initiating a software testing event by completing the JTF CapMed Software Test Request Worksheet and submitting the required form to JTF CapMed. Software sponsors are expected to be available throughout the entire test duration. The software sponsor is responsible for, but not limited to:

NOV 15 2011

- a. Completing the JTF CapMed Software Test Request Worksheet.
- b. Providing the software, licenses, and application key required for testing.
- c. Providing any specialty hardware required for software functionality.
- d. Providing software user guides required for testing.
- e. Providing the proper personnel to support testing (e.g., vendor point-of-contact, developer).

NOV 15 2011

ENCLOSURE 2PROCEDURES

1. TESTING PARAMETERS. COTS software tests are conducted against the candidate software and exercise the security of the system in its current deployment configuration. The software is tested on an FDCC imaged workstation. Hardware and operating system software configurations are examined throughout the security test process, utilizing the methods depicted throughout this Instruction.

2. ASSUMPTIONS AND CONSTRAINTS

a. A minimum of 5 days is required for performing software testing. This period does not account for any hardware, software, data, or test procedure problems encountered during the security testing. Should additional time be necessary, the Software Sponsor, JTF CapMed Lead Engineer, and Certifying Authority (CA) are immediately notified by the Test Engineer via e-mail.

b. The candidate software product operates in a secured environment in accordance with site operational and environmental procedures to ensure that risk to confidentiality, integrity, availability, and accountability of the information and network remains acceptable.

3. TESTING TOOLS. The following tools are used by JTF CapMed to assess COTS software. Additional tools may be exercised if further investigation is necessary.

a. InstallWatch. InstallWatch keeps track of all the specifics right from additions, deletions, or alterations to the directories, files and folders, initialization files, and registry information. The application facilitates the user maintaining steady records of all significant changes in the system in a number of ways, including reports or Registry entries. Details are compiled in a database for report generation.

b. System State Analyzer. System State Analyzer compares two snapshots taken at different points in time, allowing the state of a machine both before and after an application is installed to be assessed.

c. Wireshark. Wireshark is a free open-source packet analyzer. Wireshark allows the user to see all traffic being passed over the network by putting the network interface in promiscuous mode.

d. Registry Analysis_v1. Registry Analysis searches for registry additions and modifications using key phrases identified in three specific criteria files. It is an executable file for Windows. No installation, plug-ins, or supporting programs are needed.

NOV 15 2011

e. Windows scripts. Built-in Windows command utilities are scripted and run against the candidate software to gather information. Commands used include, but are not limited to, tasklist, netstat, tcpview, wmic, netstart, and netsh advfirewall.

4. SECURITY TEST APPROVAL AND SECURITY TEST BOUNDARY. In order to successfully perform the software evaluation testing, the JTF CapMed engineers utilize pre-determined methodologies and tools to measure compliance with the security requirements. The software evaluation activities include the following elements:

- a. Pre and post snapshots of the system using InstallWatch.
- b. Packet capture analysis using Wireshark.
- c. Comparison using System State Analyzer and InstallWatch.
- d. Monitoring changes to firewall, ports, and tasks using built-in Windows commands.

5. TESTING PROCESS. The security testing process includes:

- a. Submission and approval of the completed JTF CapMed Software Test Request Worksheet. The Software Sponsor (requestor) contacts the JTF CapMed Team for the worksheet. Once complete, the form is returned to the Lead Engineer for approval.
- b. Completion of the JTF CapMed software evaluation testing. The JTF Test Engineer performs testing as specified.
- c. Completion of the JTF CapMed Software Risk Assessment. The JTF Test Engineer completes the JTF CapMed Software Risk Assessment report for submission to Lead Engineer. Upon review, the report is provided to the Software Sponsor and JTF CapMed CA.
- d. Recommendation to approve or deny certification of the candidate software is provided.

6. CERTIFICATION/APPROVAL FACTORS. The issuance of a certification/approval relies on the following factors:

- a. The software must be able to operate as a COTS product.
- b. The security settings are not changed in the FDCC image.
- c. The software sufficiently protects the data type it processes.
- d. The software does not elevate any user privileges.

NOV 15 2011

- e. The software does not use or open any unapproved ports.
- f. The software can be run as a standard user.
- g. The software is not designed/developed in a foreign country.

7. VERIFICATION METHODS. The following methods are used to verify compliance throughout all levels of testing. In most cases, only one method is associated with the verification of the requirements; however, more than one method may be exercised.

a. Document Review. Review of the JTF CapMed Software Test Request Worksheet to determine if the software conforms to JTF CapMed requirements.

b. Test. The operation of the system or a part of the system using instrumentation or other test tools to collect data for analysis. For example, a number of changes to the operating system occur during installation. Data on these changes are collected for further analysis.

c. Observation. Visual examination of the operation to determine compliance.

d. Interview. Discussion between the responsible parties to ensure compliance with the requirements.

8. RISK ASSESSMENT. The JTF Software Risk Assessment Report outlines security compliance with the analyzed test results. Detailed descriptions of the test are included to adequately qualify or disqualify the candidate software for certification/approval. The final risk assessment report is provided to the Software Sponsor and JTF CapMed CA.

9. CA APPROVAL PROCESS. The CA will “certify” applications for the purposes of certification and approval for JTF CapMed-wide use, which is beneficial in that these applications will not need multiple evaluations for use in various accredited systems. Certified products are incorporated into accredited system enclaves.