



## DEFENSE INFORMATION SYSTEMS AGENCY

P.O. BOX 4502  
ARLINGTON, VIRGINIA 22204-4502

JITC INSTRUCTION 280-50-01\*

24 August 2009

### CONFIGURATION MANAGEMENT

#### JITC Configuration Management Policy

1. **Purpose.** This instruction prescribes the policy and assigns responsibility concerning configuration management for the Joint Interoperability Test Command (JITC).
2. **Applicability.** This instruction applies to all military and civilian personnel assigned to or employed by the JITC and contractors engaged in work on behalf of JITC.
3. **Authority.** CJCS Instruction 6212.01 E, Interoperability And Supportability of Information Technology and National Security Systems, 15 December 2008.
4. **References.**
  - 4.1 MIL-HDBK-61, Configuration Management, 7 February 2001.
  - 4.2 IEEE/EIA 12207.0-1996, Standard for Information Technology - Software Life Cycle Processes, March 1998.
  - 4.3 IEEE/EIA 12207.1-1997, Standard for Information Technology - Software Life Cycle Processes - Life Cycle Data, April 1998.
  - 4.4 IEEE/EIA 12207.2-1997, Standard for Information Technology - Software Life Cycle Processes - Implementation Considerations, April 1998.
  - 4.5 JITC Instruction 280-120-1, Configuration Management Plan, 9 June 2009.
  - 4.6 DoD Directive 8500.01E, Information Assurance, 23 April 2007.

4.7 DoD Instruction. 8500.2, Information Assurance Implementation, 6 February 2003.

4.8 DoD Instruction 8510.01, Information Assurance Certification and Accreditation Process, 27 November 2007.

## 5. Background.

5.1 The JITC uses a variety of Information Technology and National Security Systems (IT/NSS) and supporting test equipment, instrumentation, documentation, and office automation to accomplish its interoperability test and certification mission. Essentially all hardware, software, and firmware supporting JITC will be subjected to Configuration Management (CM) processes, which will help preclude undesirable impacts on safety, physical security, information security, quality, schedule, or cost of JITC operations.

5.2 Configuration Management requirements set forth herein are applicable to all JITC functions which are: test and certification, mission services, network support, and development programs. Systems developed internally shall comply with JITC CM requirements throughout the entire development and operational life cycle.

## 6. Policy.

6.1 The JITC will pursue an active configuration management program, in accordance with accepted configuration management practices, for all systems it develops, operates, maintains, or otherwise controls in support of JITC functions. The configuration of systems owned and operated by JITC, but provided from external sources, will be maintained through routine physical inventories and audits, and through coordination with the appropriate system manager. The configuration of systems operated by external activities will be controlled by the owning activity. The configuration of systems developed by JITC will be maintained in accordance with the references listed in Section 4 and JITC implementing instructions and plans.

6.2 All JITC test plans, reports, analysis, and/or certification documentation will include data relevant to the configuration of all items used in support of each test and/or certification effort. Software, hardware, firmware, test equipment, documentation, and other items used during JITC testing which are not maintained under a formal configuration

control program will be clearly identified as such in all test documentation. Lack of formal test equipment documentation is acceptable, as long as it is possible to re-create the test environment should it become necessary.

6.3 The JITC configuration management program will include formally documented roles, responsibilities, and procedures including management of Information Assurance documentation and information. The JITC will establish a formal Configuration Control Board (CCB) which will implement procedures to ensure a security review and approval of all proposed Department of Defense (DoD) information system changes. Interconnections to other DoD information systems will be reviewed by the CCB. The CCB will ensure that proposed system changes are adequately controlled. The CCB will further ensure by verification that the CM process is working effectively, and that unauthorized changes are not permitted or occurring.

## 7. Responsibilities.

7.1 Responsibility for JITC CM rests with the Commander. The Deputy Commander will participate in the JITC CM on an as-needed basis. Specific staff responsibilities are outlined in the following paragraphs.

7.2 Configuration Control Board. The Configuration Control Board (CCB) includes permanent members from all JITC disciplines, including those at Indian Head, Maryland. The CCB meets monthly, or as required for emergency changes. The CCB is chaired by a senior member of JITC, and reports to the Commander. The CCB will develop a standardized set of requirements for maintaining, documenting, and validating all JITC hardware, software, and infrastructure configurations. The CCB reviews and approves supplemental documents prepared by operating organizations to ensure compliance with JITC CM process requirements. The CCB tracks and consolidates JITC software capability requirements, determines priority of these requirements, and presents these findings to the JITC Corporate Board for approval and resourcing. The CCB tracks development of JITC capabilities through the CM process. Configuration Management supports the CCB by maintaining, consolidating, and tracking requirements, capabilities, and development efforts for the command, and publishes these to the entire JITC workforce.

7.3 Action Officer. The government Action Officer (AO) is delegated the responsibility and authority for a specific project to provide technical interpretation and guidance to the

contractor, via approved JITC contract tools such as JPAS. The government AO will ensure system software maintenance complies with all JITC policies and instructions. The government AO will participate and comply with JITC CCB activity as required. The AO will ensure that team leaders under their direction prepare plan supplements which address CM process compliance.

7.4 Contractor Organization. There are multiple prime contractor organizations at JITC. The following is a short description of the contractor roles and responsibilities involved in the day-to-day operations at JITC.

7.4.1 The contractor program manager is responsible for operation of the JITC C4I contract. The contractor program manager implements and maintains an organizational structure to ensure that the requirements of the government are fully understood and implemented, controlled, and documented. Contractor program managers will ensure that tasks under their jurisdiction comply with JITC CM process requirements.

7.4.2 Users are JITC testers, engineers, and others who help determine system functionality, user requirements, and design implementation. They are responsible for the presentation of the views and concerns of the hands-on users, oversight of man-machine interface, and operational capabilities of the system. Users are tasked with complying with JITC CM.

7.4.3 The CM database administrator is responsible for all databases that the CM process will use. They are responsible for assuring functionality, updates, and maintenance of all CM databases.



RONALD C. STEPHENS  
Colonel, USA  
Commander

SUMMARY OF SIGNIFICANT CHANGES. This instruction was updated primarily to reflect CM process requirements clarification which resulted from the System Readiness Review conducted at JITC in September 2008.

---

\*This instruction supersedes JITCI 280-50-01, dated 15 September 2006.

OPR: JT5B

DIST: All JITC Civilian, Military, and Contractor Personnel.