



DEFENSE
HEALTH AGENCY

PAT&IO

**OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
16401 EAST CENTRETECH PARKWAY
AURORA, CO 80011-9066**

**CHANGE 58
7950.2-M
MARCH 6, 2014**

**PUBLICATIONS SYSTEM CHANGE TRANSMITTAL
FOR
TRICARE SYSTEMS MANUAL (TSM), FEBRUARY 2008**

The TRICARE Management Activity has authorized the following addition(s)/revision(s).

CHANGE TITLE: ELIMINATION OF BENCHMARK TESTING REQUIREMENTS

CONREQ: 16623

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): This change removes references to benchmark testing.

EFFECTIVE DATE: Upon direction of the Contracting Officer.

IMPLEMENTATION DATE: Upon direction of the Contracting Officer.

This change is made in conjunction with Feb 2008 TOM, Change No. 121.

**JACOBS.KENNE
TH.C.1067162311**

Digitally signed by
JACOBS.KENNETH.C.1067162311
DN: c=US, o=U. S. Government,
ou=DoD, ou=PKI, ou=TMA,
cn=JACOBS.KENNETH.C.1067162311
Date: 2014.03.04 08:58:50 -07'00'

**Kenneth C. Jacobs
Team Chief, Performance, Analysis,
Transition, & Integration Office (PAT&IO)
Defense Health Agency (DHA)**

**ATTACHMENT(S): 2 PAGES
DISTRIBUTION: 7950.2-M**

WHEN PRESCRIBED ACTION HAS BEEN TAKEN, FILE THIS TRANSMITTAL WITH BASIC DOCUMENT.

CHANGE 58
7950.2-M
MARCH 6, 2014

REMOVE PAGE(S)

CHAPTER 1

Section 1.1, pages 23 and 24

INSERT PAGE(S)

Section 1.1, pages 23 and 24

10.1.9 Contractors shall ensure that CACs are only used by the individual to whom the CAC was issued. Individuals must protect their PIN and not allow it to be discovered or allow the use of their CAC by anyone other than him/herself. Contractors are required to ensure access to DoD systems applications and data is only provided to individuals who have been issued a CAC and whose CAC has been validated by the desktop middleware, including use of a card reader. Sharing of CACs, PINs, and other access codes is expressly prohibited.

10.1.10 The contractor shall provide the contractor locations and approximate number of personnel at each site that will require the issuance of a CAC upon contract award.

10.1.11 The contractor shall identify to Purchased Care Systems Integration Branch (PCSIB) and DMDC the personnel that require access to the DMDC Contractor Test environment in advance of the initiation of testing activities.

10.2 System Authentication

The contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers upon direction of the CO. These interfaces include, but are not limited to, the following:

- Contractor systems for inquiries and responses with DEERS
- Contractor systems and the TED Processing Center

11.0 TELECOMMUNICATIONS

11.1 MHS Demilitarized Zone (DMZ) Managed Partner Care B2B Gateway

11.1.1 For all non-DMDC web applications, the contractor will connect to a DISA-established Web DMZ. For all DMDC web applications, the contractor will connect to DMDC.

11.1.2 In accordance with contract requirements, contractors shall connect to the B2B gateway via a contractor procured Internet Service Provider (ISP) connection. Contractors will assume all responsibilities for establishing and maintaining their connectivity to the B2B Gateway. This will include acquiring and maintaining the circuit to the B2B Gateway and acquiring a Virtual Private Network (VPN) device compatible with the MHS VPN device.

11.1.3 Contractors will complete a current version of the DISA B2B gateway questionnaire providing information specific to their connectivity requirements, proposed path for the connection and last mile diagram. The completed questionnaire shall be submitted to DISA for review and scheduling of an initial technical specifications meeting.

11.2 Contractor Provided IT Infrastructure

11.2.1 Platforms shall support HyperText Transfer (Transport) Protocol (HTTP), HyperText Transfer (Transport) Protocol Secure (HTTPS), Web derived Java Applets, secure File Transfer Protocol (FTP), and all software that the contractor proposes to use to interconnect with DoD facilities.

11.2.2 Contractors shall configure their networks to support access to government systems (e.g., configure ports and protocols for access).

11.2.3 Contractors shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable.

11.3 System Authorization Access Request (SAAR) Defense Department (DD) Form 2875

11.3.1 All contractors that use the DoD gateways to access government IT systems and/or DoD applications (e.g., DEERS applications, PEPR, DCS, MDR, etc.) must submit the most current version of DD Form 2875 found on the DISA web site: <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo3211.html> in accordance with CO guidance. A DD Form 2875 is required for each contractor employee who will access any system and/or application on a DoD network. The DD Form 2875 must clearly specify the system and/or application name and justification for access to that system and/or application.

11.3.2 Contractors shall complete and submit the completed DD Form 2875 to the TMA Privacy Office for verification of ADP Designation (see [paragraph 5.0](#)). The TMA Privacy Office will verify that the contractor employee has the appropriate background investigation completed/or a request for background investigation has been submitted to the OPM. Acknowledgement from OPM that the request for a background investigation has been received and that an investigation has been scheduled will be verified by the TMA Privacy Officer prior to access being approved.

11.3.3 The TMA Privacy Office will forward the DD Form 2875 to the TIMPO for processing; TIMPO will forward DD Form 2875s to DISA. DISA will notify the user of the ID and password via e-mail upon the establishment of a user account. User accounts will be established for individual use and may not be shared by multiple users or for system generated access to any DoD application. Misuse of user accounts by individuals or contractor entities will result in termination of system access for the individual user account.

11.3.4 Contractors shall conduct a monthly review of all contractor employees who have been granted access to DoD IS/networks to verify that continued access is required. Contractors shall provide the TMA Privacy Office with a report of the findings of their review by the 10th day of the month following the review. Reports identifying changes to contractor employee access requirements shall include the name, SSN, Company, IS/network for which access is no longer required and the date access should be terminated.

11.4 MHS Systems Telecommunications

11.4.1 The primary communication links shall be via Secure Internet Protocol (IPSEC) VPN tunnels between the contractor's primary site and the MHS B2B Gateway.

11.4.2 The contractor shall place the VPN appliance device outside the contractor's firewalls and shall allow full management access to this device (e.g., in router access control lists) to allow Central VPN Management services provided by the DISA or other source of service as designated by the MHS to remotely manage, configure, and support this VPN device as part of the MHS VPN domain.