



DEFENSE
HEALTH AGENCY

PAT&IS

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

**CHANGE 79
7950.2-M
OCTOBER 16, 2015**

**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: TESTTRACK DEFINITION

CONREQ: 17471

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): This change replaces the term "TestTrack Pro" with the more generic term, "Government defined application."

EFFECTIVE DATE: November 16, 2015.

IMPLEMENTATION DATE: November 16, 2015.

LOZOYA.JOSE
.L.1231416397
Digitally signed by
LOZOYA.JOSE.L.1231416397
DN: c=US, o=U S. Government,
ou=DoD, ou=PKI, ou=DHA,
cn=LOZOYA.JOSE.L.1231416397
Date: 2015.10.14 12:20:16 -06'00'

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

**ATTACHMENT(S): 4 PAGES
DISTRIBUTION: 7950.2-M**

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

CHANGE 79
7950.2-M
OCTOBER 16, 2015

REMOVE PAGE(S)

CHAPTER 1

Section 1.1, pages 3, 4, 19, and 20

INSERT PAGE(S)

Section 1.1, pages 3, 4, 19, and 20

- DoD 5015.2-D, "Records Management Program," March 6, 2000
- DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004
- Federal Information Processing Standards Publication 201 (FIPS 201-1), "Personal Identify Verification (PIV) of federal Employees and Contractors," March 2006
- Directive Type Memorandum (DTM) 08-006, "DoD Implementation of Homeland Security Presidential Directive-12 (HSPD-12)," November 26, 2008
- DoDI 8582.01, "Security of Unclassified DoD Information on Non-DoD Information Systems"

The requirements above shall be met by contractors, subcontractors and other individuals who have access to IS containing PII protected by the Privacy Act of 1974 and PHI under HIPAA.

2.0 SYSTEM INTEGRATION, IMPLEMENTATION AND TESTING MEETINGS

2.1 The DHA hosts regularly scheduled meetings, via teleconference, with contractor and government representatives. Government attendees may include, but are not limited to Defense Manpower Data Center (DMDC), Infrastructure & Operations Division (I&OD), and Defense Information System Agency (DISA). The purpose of these meetings is to:

- Review the status of system connectivity and communications.
- Identify new DEERS applications or modifications to existing applications, e.g., DEERS On-line Enrollment System (DOES).
- Issue software enhancements.
- Implement system changes required for the implementation of new programs and/or benefits.
- Review data correction issues and corrective actions to be taken (e.g., catastrophic cap effort--review, research and adjustments).
- Monitor results of contractor testing efforts.
- Other activities as appropriate.

2.2 DHA provides a standing agenda for the teleconference with the meeting announcement. Additional subjects for the meetings are identified as appropriate. Contractors are required to ensure representatives participating in the calls are subject matter experts for the identified agenda items and are able to provide the current status of activities for their organization. The contractor **shall** ensure testing activities are completed within the scheduled time frames and any

problems experienced during testing are reported via the Government defined application for review and corrective action by DHA or their designee. Upon the provision of a corrective action strategy or implementation of a modification to a software application by DHA (to correct the problem reported by the contractor), the contractor is responsible for retesting the scenario to determine if the resolution is successful. Retesting shall be accomplished within the agreed upon time frame. The contractor shall update the Government defined application upon completion of retesting activities.

2.3 DHA will also document system issues and deficiencies into the Government defined application related to testing and production analysis of the contractors systems and processes. Upon the provision of a corrective action strategy or implementation of a modification to a software application by the contractor (to correct the problem reported by DHA), the contractor shall retest the scenario to determine if the resolution is successful. Retesting shall be accomplished within the agreed upon time frame. The contractor shall correct internal system problems that negatively impact their interface with the Business to Business (B2B) Gateway, Military Health System (MHS), DMDC, etc. and/or the transmission of data, at their own expense.

2.4 Each organization identified shall provide two Points of Contact (POCs) to DHA to include telephone and e-mail contact and will be used for call back purposes, notification of planned and unplanned outages and software releases. POCs will be notified via e-mail in the event of an unplanned outage using the POC notification list, so it is incumbent upon each organizations to notify DHA of changes to the POC list.

3.0 ADP REQUIREMENTS

It is the responsibility of the contractor to employ adequate hardware, software, personnel, procedures, controls, contingency plans, and documentation to satisfy DHA data processing and reporting requirements. Items requiring special attention are listed below.

3.1 Continuity of Operations Plan (COOP)

3.1.1 The contractor shall develop a single plan, deliverable to the DHA CO on an annual basis that ensures the continuous operation of their Information Technologies (IT) systems and data support of TRICARE. The plan shall provide information specific to all actions that will be taken by the prime and subcontractors in order to continue operations should an actual disaster be declared for their region. The COOP shall ensure the availability of the system and associated data in the event of hardware, software and/or communications failures. The COOP shall also include prime and subcontractor's plans for relocation/recovery of operations, timeline for recovery, and relocation site information in order to ensure compliance with the TOM, Chapters 1 and 6. Information specific to connection to the B2B Gateway to and from the relocation/recovery site for operations shall also be included in the COOP. For relocation/recovery sites, contractors must ensure all security requirements are met and appropriate processes are followed for the B2B Gateway connectivity. The contractor's COOP will enable compliance with all processing standards as defined in the TOM, Chapter 1, and compliance with enrollment processing and Primary Care Manager (PCM) assignment as defined in TOM, Chapter 6. The COOP should include restoration of critical functions such as claims and enrollment within five days of the disaster. The government reserves the right to re-prioritize the functions and system interactions proposed in the COOP during the review and approval process for the COOP.

8.1.6 Personal Identification Number (PIN) Resets

Should an individual's CAC become locked after attempting three times to access it, the PIN will have to be reset at a RAPIDS facility or by designated individuals authorized CAC PIN Reset (CPR) applications. These individuals may be contractor personnel, if approved by the government representative. PIN resets cannot be done remotely. The government will provide CPR software licenses and initial training for the CPR process; the contractor is responsible for providing the necessary hardware for the workstation (PC, Card Readers, Fingerprint capture device). It is recommended that the CPR workstation not be used for other applications, as the government has not tested the CPR software for compatibility. The CPR software must run on the desktop and cannot be run from the Local Area Network (LAN). The contractor shall install the CPR hardware and software, and provide the personnel necessary to run the workstation.

8.1.7 E-Mail Address Change

The User Maintenance Portal (UMP) is an available web service that allows current CAC holders to change e-mail signing and e-mail encryption certificates in the event of a change in e-mail addresses. This service is accessible from a local workstation via web services.

8.1.8 System Requirement for CAC Authentication

Contractors shall procure, install, and maintain desktop level CAC readers and middleware. The middleware software must run on the desktop and cannot be run from the LAN. Technical Specifications for CACs and CAC readers may be obtained at <http://www.dmdc.osd.mil/smartcard>.

8.1.9 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.

8.1.10 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.

8.1.11 The contractor shall identify to DHA and DMDC the personnel that require access to the DMDC Contractor Test environment in advance of the initiation of testing activities.

8.2 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

9.0 TELECOMMUNICATIONS

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

9.1.1 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.

9.1.2 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.

9.1.3 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.

9.2 Contractor Provided IT Infrastructure

9.2.1 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.

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

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

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

9.3.1 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.

9.3.2 Contractors shall complete and submit the completed DD Form 2875 to the DHA Privacy Office for verification of ADP Designation. The DHA 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. Acknowledgment from OPM that the request for a background investigation has been received and that an investigation has been scheduled will be verified by the DHA Privacy Officer prior to access being approved.