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

CHANGE 100
7950.2-M
DECEMBER 20, 2017

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

The Defense Health Agency has authorized the following addition(s)/revision(s).

CHANGE TITLE: CAC EMAIL CERTIFICATION

CONREQ: 18460

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): This change adds new policy guidance per DMDC policy requiring all CACs to use only government approved e-mail address certificates, from time of issuance.

EFFECTIVE DATE: January 6, 2017.

IMPLEMENTATION DATE: January 22, 2018.

ARENDALE, J
OHN, LOUIS, I
I. 1150775368
Digitally signed by
ARENDALE. JOHN LO
U.S. I. 1150775368
Date: 2017.12.14
13:55:28 -07'00'

John L. Arendale
Director, Health Plan Operations
Division (HPOD)
Defense Health Agency (DHA)

WHEN PRESCRIBED ACTION HAS BEEN TAKEN, FILE THIS TRANSMITTAL WITH BASIC DOCUMENT.
CHAPTER 1

Section 1.1, pages 13 through 25

Section 1.1, pages 13 through 26
5.5.4 Requests for Additional Information

PSB may require additional information while the contractor employee’s investigation is in progress. The FSO will be notified to provide the information by a specified date or the investigation may be rejected or returned unacceptable. The FSO shall review applications for required information prior to release, to reduce case rejections and requests for additional information.

5.5.5 Notification of Employee Termination and Unfavorable Personnel Security Determination

5.5.5.1 The FSO shall notify PSB immediately when a contractor employee is terminated from a DHA contract. E-mail notification shall include the employee’s name and termination date. If a contractor moves an employee to another DHA contract, PSB shall be notified immediately, especially when a contractor employee is being moved from an unclassified contract to a classified contract.

5.5.5.2 PSB will notify the FSO by e-mail when a contractor employee has received an unfavorable personnel security determination. Upon receipt of a denial letter from PSB, the FSO shall immediately terminate the employee’s access to DoD IT systems. The return receipt letter and the denial letter from PSB are attached to the e-mail notification from PSB. The return receipt letter shall be returned to PSB no later than one week after receipt, to verify compliance with termination of the employee’s access.

5.5.6 Transfers Between Contractors

When contractor employees transfer employment from one DHA contractor to another DHA contractor while their investigation for ADP/IT trustworthiness determination is in process, the scheduled investigation may be applied to the new employing contractor. It shall be the responsibility of the new employer to provide notification to PSB when this type of transfer occurs. The notification shall contain employee’s name and effective date of transfer.

5.5.7 Notification and Mailing

The contractor shall process sensitive information according to applicable laws and DoD policies related to privacy and confidentiality. The contractor shall transmit PII or PHI via encrypted e-mail or the OPM secure portal. The contractor shall use the following information to contact the PSB.

Mailing Address:
Defense Health Agency
ATTN: Personnel Security Branch
7700 Arlington Blvd., Suite 5101
Falls Church, VA 22042-5101

e-QIP Helpdesk: (703) 681-6508
5.6 References

- DoDD 5136.01, “Assistant Secretary of Defense for Health Affairs (ASD(HA)),” September 30, 2013.

- DoDD 5136.13, “Defense Health Agency (DHA).”


6.0 PUBLIC KEY INFRASTRUCTURE (PKI)

The DoD has initiated a PKI policy to support enhanced risk mitigation strategies in support of the protection of DoD’s system infrastructure and data. DoD’s implementation of PKI requirements are specific to the identification and authentication of users and systems within DoD (DoDI 8520.02). The following paragraphs provide current DoD PKI requirements.

6.1 User Authentication

All contractor personnel accessing DoD applications and networks shall obtain PKI enabled and Personal Identity Verification (PIV) compliant Government accepted credentials. Contractor personnel with access limited to internal contractor systems and applications are not required to obtain PKI enabled and PIV compliant credentials. Such credentials shall follow the PIV trust model (FIPS 201-2) and be acceptable to the government. Currently, to meet this requirement, contractor employees shall obtain Government-issued CACs. PIV compliant credentials are required for access to DoD systems, networks and data. Alternate sign on access will not be granted. Encryption and digital signatures shall be used for information transmitted electronically that includes DoD/DHA data covered by the Privacy Act, HIPAA and SI and network requirements.
6.1.1  Common Access Card (CAC) Issuance

6.1.1.1  The CAC is the standard identification for Service members, DoD civilian employees, and eligible DoD contractor personnel. It is the principal card used to enable both physical access to a DoD facility and access, via logon, to DoD networks on-site or remotely. Access to the DoD network requires the use of a computer with Government-controlled configuration or use of a DoD-approved remote access procedure in accordance with the DISA Security Technical Implementation Guide (DISA STIG).

6.1.1.2  Trust Associated Sponsorship System (TASS) is a web-based system that allows eligible DoD contractors to apply for a CAC through the Internet. Government sponsors (also known as Trusted Agent (TA)) approve the application to receive government credentials.

6.1.1.3  CACs Issued On Or After January 6, 2017

CACs issued, reissued, or replaced on or after January 6, 2017, will be issued with a blank e-mail certificate unless the CAC holder already has a DoD approved e-mail address. Instructions for requesting an approved e-mail address are available in paragraph 6.1.1.3.3. Without an approved government e-mail address (and the accompanying DoD e-mail certificate), the CAC holder will be unable to use the capabilities afforded by such a certificate, including digital signatures, digital encryption, and/or to access government systems that require a DoD approved e-mail certificate authentication. CAC capabilities that do not require a DoD approved e-mail certificate for authentication will still function. If a CAC owner requires a DoD approved e-mail certificate to perform their duties, the DHA’s DoD approved e-mail is Defense Enterprise Email (DEE). Not all contractors require DoD approved e-mail certificates on their CAC to perform those duties. More information is provided in paragraph 6.1.1.3.2 or the contractor shall reference the specific requirements outlined in the contract for clarification.

6.1.1.3.1  E-mail Address Certificates on CACs

6.1.1.3.2  CAC owners will require an approved DoD e-mail address certificate on their CAC in order to perform certain functions, such as the ability to digitally sign, digitally encrypt, and/or access government systems that require a DoD approved e-mail address certificate assigned and the e-mail address certificate will remain blank. Some current CAC users may already have another type of e-mail certificate that complies with DoD requirements. If a contractor requires the capabilities afforded by a DoD approved e-mail certificate on their CAC, they shall obtain a DEE account, as described below. The DEE account provides the CAC holder with the necessary DoD approved e-mail certificates needed for the CAC. It also creates an e-mail in-box that allows the user to send/receive encrypted e-mails and send/receive government correspondence, among other capabilities. Once a CAC holder obtains their DEE account, the account may be accessed using Outlook Web Access (OWA) at https://web.mail.mil.

6.1.1.3.3  The Contracting Officer’s Representative/Program Manager (COR/PM) will e-mail the contractor’s FSO requesting a list of users’ first and last names, persona type codes (Civilian, Military, Contractor) and DoD Identification (ID) Number, located on the back of the user’s CAC be provided to the COR. Upon receipt, the COR/PM will forward the information to Global Service Center (GSC) DHA.ITCallCenter@mail.mil requesting DEE accounts be provided for each user listed. A DHA Add User Form is not required to only obtain DEE accounts for CAC owners. GSC will create a DEE account for each contractor request submitted, and provide the COR/PM acknowledgment of
the account creation. The COR/PM will forward the account information to the FSO, who shall provide the CAC owners the new account information with instructions on how to create or update their DEERS/Real-Time Automated Personnel ID System (RAPIDS) Online profiles as described below.

6.1.1.3.4 When the CAC holder receives their DEE account information, they shall:

- Update the e-mail certificate associated with their CAC:
  - Sign in to the following link (do not select the DoD EMAIL certificate option):
    https://www.dmdc.osd.mil/self_service/rapids/unauthenticated?execution=e1s1
  - Within CAC Maintenance, select Change CAC E-mail.
  - Update the DoD approved e-mail address on the CAC to reflect the DEE (@mail.mil) account. This will create the DoD Certs needed for the digital signature and encryption. (This may take up to 72 hours for the settings to update and be reflected in the system.)

- Update their Global Address List (GAL) properties:
  - Sign in to the following link: https://www.dmdc.osd.mil/milconnect/
  - Select Update Work Contact Info (GAL).
  - Update contact information accordingly.
  - Access their DEE account using OWA at https://web.mail.mil.

**Note:** The amount of time required to obtain a DEE account is contingent upon the independent steps performed by the parties outlined above. Activities are typically completed in hours.

6.1.2 FSO Roles and Responsibilities

6.1.2.1 Obtaining a CAC

The FSO shall:

- Identify contractor support personnel who require a CAC for accessing DoD networks and facilities.

- Verify the applicant’s background investigation by submitting a request to PSB.

- Complete Sections I and III of the DHA Form 33, for the initial and/or renewal CAC.

- Submit the form (DHA Form 33) to the COR for approval.

- Fax the completed form to (703-681-5207) ATTN: PSB/-TASS/Common Access Card Branch (CACB) or e-mail to (dha.ncr.security.mbx.personnel-security-tass@mail.mil).
6.1.2.2 Obtaining E-Mail Address Certificate

The FSO shall:

- Assist the CAC owner with obtaining a DoD approved e-mail address (and the accompanying e-mail certificate) for their CAC, if one is required to perform their job duties.

- Submit to the COR a list of user’s first and last names, persona type codes (Civilian, Military, Contractor) and DoD ID Number, for those requiring an e-mail certificate.

6.1.2.3 Out-Processing Procedures

The FSO shall:

- Establish out-processing procedures to collect the CAC when an employee quits, is terminated from the company, or when the CAC is no longer required.

- Notify the TA to revoke the employee’s CAC.

- CACs shall be returned in accordance with paragraph 6.1.3.8.

6.1.3 CAC Guidelines and Restrictions

6.1.3.1 Any person willfully altering, damaging, lending, counterfeiting, or using these cards in any unauthorized manner is subject to fine or imprisonment or both, as prescribed in sections 499, 506, 509, 701, and 1001 of title 18, United States Code (USC). Section 701 prohibits photographing or otherwise reproducing or possessing DoD ID cards in an unauthorized manner, under penalty of fine or imprisonment or both. Unauthorized or fraudulent use of ID cards would exist if bearers used the card to obtain benefits and privileges to which they are not entitled. Examples of authorized photocopying include photocopying of DoD ID cards to facilitate medical care processing, check cashing, voting, tax matters, compliance with appendix 501 of title 50, USC (also known as “The Service member’s Civil Relief Act”), or administering other military-related benefits to eligible beneficiaries. Whenever possible, the ID card shall be electronically authenticated in lieu of photographing the card.

6.1.3.2 CACs shall not be amended, modified, or overprinted by any means. No stickers or other adhesive materials are to be placed on either side of an ID card. Holes shall not be punched into ID cards.

6.1.3.3 Access

The granting of access is determined by the contractor or system owner as prescribed by the DoD.

6.1.3.4 Accountability

CAC holders shall maintain accountability of their CACs at all times while affiliated with the DoD contractor, or until surrendered in accordance with paragraphs 6.1.3.7 and 6.1.3.8.
6.1.3.5 Multiple Cards

In instances where an individual has been issued more than one CAC (e.g., an individual that is eligible for a CAC as both a Reservist and as a contractor employee), only the CAC that most accurately depicts the capacity in which the individual is affiliated with the DoD should be utilized at any given time.

6.1.3.6 Renewal and Expiration

CACs may be renewed 90 days prior to the CAC expiration date. The CAC will be issued for three years or until the contract end date, whichever is shorter.

6.1.3.7 Replacement

Within 24 hours of becoming aware of the loss of a CAC, the contractor shall provide the RAPIDS issuance site a letter from the FSO confirming the CAC has been reported lost, stolen, confiscated, or destroyed, along with a copy of a valid (unexpired) State or Federal Government-issued picture ID.

6.1.3.8 Retrieval

The CAC is property of the U.S. Government and shall be retrieved from the contractor employee if the ID has expired, or is damaged or compromised. Additionally, CACs shall be retrieved if the employee is no longer affiliated with the DoD contractor or no longer meets the eligibility requirements for the card. The CAC shall be returned to the following address within one week using FedEx Delivery service:

Defense Health Agency
Mission Assurance Division
Personnel Security Branch
ATTN: TASS/CACB
7700 Arlington Blvd, Suite 5101
Falls Church, VA 22042-5101

6.1.4 Personal Identification Number (PIN) Resets

Should an individual’s CAC become locked after attempting three times to access it, the PIN shall 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 shall provide the necessary hardware for the workstation (PC, Card Readers, Fingerprint capture device). The CPR workstation shall 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.
6.1.5 System Requirements for CAC Authentication

The contractor 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 https://www.dmdc.osd.mil/appj/dwp/contractor_civ_roles.jsp.

6.1.6 The contractor 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. The contractor shall 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.

6.1.7 The contractor shall provide the contractor locations and approximate numbers of personnel at each site who will require the issuance of a CAC upon contract award.

6.1.8 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.

6.2 System Authentication

The contractor shall 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

7.0 TELECOMMUNICATIONS

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

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

7.1.2 In accordance with contract requirements, the contractor shall connect to the B2B gateway via a contractor procured Internet Service Provider (ISP) connection. The contractor shall 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.

7.1.3 The contractor shall 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.
7.2 Contractor Provided IT Infrastructure

7.2.1 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.

7.2.2 The contractor shall configure their networks to support access to government systems (e.g., configure ports and protocols for access).

7.2.3 The contractor shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable.

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

7.3.1 All contractors that use the DoD gateways to access government IT systems and/or DoD applications (e.g., DEERS applications, PEPR, DCS, MDR, etc.) shall submit the most current version of DD Form 2875 found on the DISA web site: http://www.dtic.mil/whs/directives/forms/eforms/dd2875.pdf in accordance with CO guidance. A DD Form 2875 shall be completed 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.

7.3.2 The contractor 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.

7.3.3 The DHA Privacy Office will forward the DD Form 2875 to I&OD for processing; I&OD 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.

7.3.4 The contractor 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. The contractor shall provide the DHA 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, DoD ID number from CAC, Company, IS/network for which access is no longer required and the date access should be terminated.

7.4 MHS Systems Telecommunications

7.4.1 The primary communication links shall be via Secure Internet Protocol (IPSEC) VPN tunnels between the contractor’s primary site and the MHS B2B Gateway.
7.4.2 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.

7.4.3 For backup purposes, an auxiliary VPN device for contractor locations shall also be procured and configured for operation to minimize any downtime associated with problems of the primary VPN.

7.4.4 Devices sent by the contractor to the MHS VPN management authority (e.g., DISA) will be sent postage paid and include prepaid return shipping arrangements for the devices(s).

7.4.5 The MHS VPN management authority (e.g., DISA) will remotely configure the VPN once installed by the contractor.

7.4.6 Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the contractor. Troubleshooting of VPN equipment will be the responsibility of the government.

7.5 Establishment of Telecommunications

7.5.1 Telecommunications shall be established with the MHS through coordination with DHA, I&OD, and DISA. The contractor shall identify their requirement(s) for the establishment of telecommunications with the MHS, DMDC or other Government entity.

7.5.2 The contractor shall complete the current version of the B2B Gateway Questionnaire (to be provided by DHA) identifying the required telecommunication infrastructure between the contractor and the MHS systems. This includes all WAN, LAN, VPN, Web DMZ, and B2B Gateway access requirements. The completed Questionnaire shall be returned to the DHA designated POC for review and approval. Upon Government request, the contractor shall provide technical experts to provide any clarification of information provided in the Questionnaire. DHA will forward the Questionnaire to I&OD for further review and processing.

7.5.3 I&OD will coordinate any requirements for additional information with the DHA POC and schedule any meetings required to review the Questionnaire. Upon approval of the Questionnaire, I&OD will coordinate a testing meeting with DHA. DHA will notify the contractor POC of the meeting schedule. The purpose of the testing meeting is to complete a final review of the telecommunication requirements and establish testing dates.

7.5.4 The contractor shall provide the DHA with a copy of the approved and signed B2B Questionnaire for all telecommunication efforts.

7.6 Contractors Located On Military Installations

7.6.1 Contractors located on a military installation who require direct access to government systems shall coordinate/obtain these connections with the local MTF and Base/Post/Camp communication personnel. These connections will be furnished by the government.
7.6.2 Contractors located on military installations that require direct connections to their networks shall provide an isolated IT infrastructure. They shall coordinate with the Base/Post/Camp communications personnel and the MTF in order to get approval for a contractor procured circuit to be installed and to ensure the contractor is within compliance with the respective organizational security policies, guidance and protocols.

**Note:** In some cases, the contractor may not be allowed to establish these connections due to local administrative/security requirements.

7.6.3 The contractor shall be responsible for all security certification documentation as required to support DoD IA requirements for network interconnections. Further, the contractor shall provide, on request, detailed network configuration diagrams to support IA accreditation requirements. The contractor shall comply with IA accreditation requirements. All network traffic shall be via TCP/IP using ports and protocols in accordance with current Service security policy. All traffic that traverses MHS, DMDC, and/or military Service Base/Post/Camp security infrastructure is subject to monitoring by security staff using Intrusion Detection Systems.

7.7 DHA/TED

7.7.1 Primary Site

The TED primary processing site is currently located in Oklahoma City, OK, and operated by the Defense Enterprise Computing Center (DECC), Oklahoma City Detachment of the DISA.

**Note:** The location of the primary site may be changed. The contractor shall be advised should this occur.

7.7.2 General

The common means of administrative communication between government representatives and the contractor is via telephone and e-mail. An alternate method may be approved by DHA, as validated and authorized by DHA. Each contractor on the telecommunication network is responsible for furnishing to DHA at the start-up planning meeting (and update when a change occurs), the name, address, and telephone number of the person who will serve as the technical POC. The contractor shall also furnish a separate computer center (Help Desk) number to DHA which the DHA computer operator may use for resolution of problems related to data transmissions.

7.7.3 TED-Specific Data Communications Technical Requirements

The contractor shall communicate with the government’s TED Data Center through the MHS B2B Gateway.

7.7.3.1 Communication Protocol Requirements

7.7.3.1.1 File transfer software shall be used to support communications with the TED Data Processing Center. CONNECT:Direct is the current communications software standard for TED transmissions. The contractor shall upgrade/comply with any changes to this software. The
The contractor shall provide this product and a platform capable of supporting this product with the TCP/IP option included. Details on this product can be obtained from:

Sterling Commerce  
4600 Lakehurst Court  
P.O. Box 8000  
Dublin OH 43016-2000 USA  
Phone: 614-793-7000  
Fax: 614-793-4040

7.7.3.1.2 For Ports and Protocol support, TCP/IP communications software incorporating the TN3270 emulation shall be provided by the contractor.

7.7.3.1.3 Transmission size is limited to any combination of 400,000 records at one time.

7.7.3.1.4 “As Required” Transfers

Ad hoc movement of data files shall be coordinated through and executed by the network administrator or designated representative at the source file site. Generally speaking, the requestor needs only to provide the POC at the remote site, and the source file name. Destination file names shall be obtained from the network administrator at the site receiving the data. Compliance with naming conventions used for recurring automated transfers is not required. Other site specific requirements, such as security constraints and pool names are generally known to the network administrators.

7.7.3.1.5 File Naming Convention

7.7.3.1.5.1 All files received by and sent from the DHA data processing site shall comply with the following standard when using CONNECT:Direct:

<table>
<thead>
<tr>
<th>POSITION(S)</th>
<th>CONTENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - 2</td>
<td>“TD”</td>
</tr>
<tr>
<td>3 - 8</td>
<td>YYMMDD Date of transmission</td>
</tr>
<tr>
<td>9 - 10</td>
<td>Contractor number</td>
</tr>
<tr>
<td>11 - 12</td>
<td>Sequence number of the file sent on a particular day. Ranges from 01 to 99. Reset with the first file transmission the next day.</td>
</tr>
</tbody>
</table>

7.7.3.1.5.2 All files sent from the DHA data processing site shall be named after coordination with receiving entities in order to accommodate specific communication requirements for the receivers.

7.7.3.1.6 Timing

Under most circumstances, the source file site shall initiate automated processes to cause transmission to occur. With considerations for timing and frequency, activation of transfers for each application shall be addressed on a case by case basis.
7.7.3.1.6.1 Alternate Transmission

Should the contractor not be able to transmit their files through the normal operating means, the contractor shall notify DHA (EIDS Operations) to discuss alternative delivery methods.

7.8 DHA/MHS Referral And Authorization System

The MHS Referral and Authorization System is to be determined. Interim processes are discussed in the TOM.

7.9 DHA/TRICARE Duplicate Claims System

The DCS is planned to operate as a web application. The contractor shall provide internal connectivity to the public Internet. The contractor is responsible for all systems and operating system software needed internally to support the DCS. (See the TOM, Chapter 9 for DCS Specifications.)

7.10 Payroll Allotment Systems

Enrollment fees/premium payments for specified TRICARE Programs may be paid by electronic monthly allotments from military payroll. The availability of this payment option is determined by the Program requirements and the service member's duty status and may not be available for all TRICARE Programs. Payroll allotment data is exchanged between military payroll centers and the TRICARE purchased care contractors. TRICARE contractors process allotment information exchanged with military payroll centers in accordance with the TOM, Chapter 6, Section 1. The following allotment processing guidance is provided in accordance with the Memorandum of Understanding (MOU) established between the DHA and Defense Finance and Accounting Service (DFAS), the U.S. Coast Guard (USCG), and Public Health Service (PHS) for allotments from retired pay.

7.10.1 Exchange of Payroll Allotment Data

The contractor shall exchange payroll allotment data with the DFAS and the USCG and PHS using a specified transmission protocol.

7.10.1.1 DFAS

Payroll allotment data for the U.S. Army, Air Force, Navy, and Marines must be transmitted to DFAS via the B2B Gateway using Secure File Transfer Protocol (SFTP) or a secure internet file transfer, e.g., Multi-Host Internet Access Portal (MIAP). The use of the B2B or a Government identified secure file transfer requires compliance with all security requirements in this Chapter. The contractor shall separately provide DFAS with a System Authorization Access Request (SAAR) DD Form 2875 requesting access to DFAS systems. This is in addition to what may have already been submitted for access to the B2B.
7.10.1.2 USCG and PHS

Payroll allotment data for the USCG and PHS shall be transmitted via the SilkWeb (a secure Internet file transfer protocol) and Titan web application (see instructions in Addendum C). All security and data handling requirements in this Chapter remain in effect. In addition, contractor shall obtain user IDs and passwords from the designated POC at the PHS.

7.10.2 Data Transmission Requirements

7.10.2.1 The contractor shall provide DFAS/USCG/PHS with a monthly file of retirees who have selected TRICARE Prime for their health benefit and elected monthly allotments as the methodology for paying enrollment fees. DFAS will return feedback files to the contractor providing determinations of the actions, acceptance or rejection and whether the item is paid or unpaid.

7.10.2.2 The contractor shall provide DFAS/USCG/PHS with POCs for testing, system and ongoing business requirements. POC information shall be maintained and include: name, title, contractor name, address, electronic mail address and telephone number. Updated information shall be provided to DFAS when the POC or contact information changes.

7.10.2.3 DFAS/USCG/PHS will provide the contractor with start/stop and change allotment requests received directly from TRICARE beneficiaries. The contractor shall process these requests and submit an initial file containing information for all allotments selected in time for the first submission. Subsequent files will contain only new allotments and stops and/or changes.

7.10.2.4 The file (initial and subsequent) shall be sent using the appropriate transmission protocol determined by the receiving payroll center, e.g., DFAS or USCG/PHS.

7.10.2.5 The contractor shall submit an electronic mail notification to DFAS/USCG/PHS notifying them of the file transmission.

7.10.3 File Layout

7.10.3.1 The contractor shall exchange the following files with DFAS:

- Input data
- Reject Report
- Deduction Report

7.10.3.2 The file layout is provided at Addendum C. The contractor will be notified of any changes to the file layout by the CO.

7.10.3.3 The contractor shall submit files using the naming convention designated by DFAS.

7.10.4 Data Transmission Schedule

7.10.4.1 Data shall be transmitted by the contractor or their designated subcontractor on the business day immediately prior to the eighth day of each month (or on the previous Thursday, should the eighth fall on a Saturday or Sunday), for allotments due on the first day of the upcoming
month. The only exception to this schedule is for the month of December when all data shall be transmitted so it is received on the first business day of December.

7.10.4.2 During months when no monthly beneficiary data exists, the contractor shall continue to submit a file without data in accordance with the eighth day of the month rule. The file shall consist of a header and trailer record with no data in between. The electronic mail notification shall indicate the file contains no member data.

7.10.4.3 Within 24 hours of file processing by DFAS/USCG/PHS, the contractor will receive a file from the pay center identifying all “rejected” submissions and the reasons for the rejection. The contractor shall research the rejected submissions and resubmit resolved transactions on the following month's file. The contractor shall also notify the beneficiary in accordance with TOM, Chapter 6, Section 1.

7.10.4.4 The contractor will receive a file of the “deduct/no deduct” file that contains the “no deduct” reasons following processing of the ‘compute pay cycle’ by the pay center. The contractor shall research these items and resubmit resolved items, as appropriate, on the following month's file. The “deduct/no deduct” file is informational and will document all payments not collected as well as unfulfilled allotment requests (e.g., insufficient pay to cover deduction).

7.10.4.5 The contractor's banking institution will receive a Corporate Trade Exchange (CTX) “payment” file from DFAS on the first business day of the month following the submission of the files.

7.10.5 Data Transmission Start Up

7.10.5.1 The DHA will coordinate B2B Gateway and DFAS connectivity for all contractors.

7.10.5.2 DHA will also coordinate integration testing of the connectivity and data transmission. DHA and the contractor will collaborate with DFAS/USCG/PHS on the development of a test plan and schedule.

7.10.6 Transition

7.10.6.1 Upon reprocurement of a TRICARE contract, an incumbent contractor may succeed itself or a new contract company may be awarded the contract. Therefore, DHA will coordinate transition activities with the contractor and DFAS/USCG/PHS during the transition-in period (see the TOM, Chapter 1, Section 7). When the contract is awarded to a new company, the following actions will be taken by the outgoing and incoming contractors.

7.10.6.2 The outgoing contractor shall send a “stop” (allotment) for any beneficiary whose transfer (disenrollment) has been processed by the sixth day of the month in which the file is being created.

7.10.6.3 The incoming contractor shall send a “start” (allotment) for any beneficiary whose transfer (enrollment) has been processed by the sixth of each month that the file is being created.

- END -