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

DEFENSE
HEALTH AGENCY

HPOD

CHANGE 99
7950.2-M
NOVEMBER 27, 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: **NIST SPECIAL PUBLICATION 800-171 CHECKLIST**

CONREQ: 18771

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): This change updates the NIST SP 800-53 Checklist to the NIST SP 800-171 Checklist and deletes references not pertaining to non-DoD entities.

EFFECTIVE DATE: December 31, 2017.

IMPLEMENTATION DATE: December 31, 2017.

ARENDALE.JOHN.LOUIS.II.1150775368
Digitally signed by ARENDALE.JOHN.LOUIS.II.1150775368
Date: 2017.11.17 15:33:04 -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.

REMOVE PAGE(S)	INSERT PAGE(S)
CHAPTER 1	
Section 1.1, pages 5 through 25	Section 1.1, pages 5 through 25

3.2 Security Requirements

3.2.1 The contractor shall ensure security and access requirements are met in accordance with existing contract requirements for all COOP and disaster recovery activities. Waivers of security and access requirements will not be granted for COOP or disaster recovery activities.

3.3 Annual Disaster Recovery Tests

3.3.1 The prime contractor will coordinate annual disaster recovery testing of the COOP with its subcontractor(s) and the government. Coordination with the government will begin NLT 90 days prior to the requested start date of the disaster recovery test. Each prime contractor will ensure all aspects of the COOP are tested and coordinated with any contractors responsible for the transmission of TRICARE data. Each prime contractor must ensure major TRICARE functions are tested.

3.3.2 The prime contractor shall also ensure testing support activities (e.g., DEERS, TED, etc.) are coordinated with the responsible government POC NLT 90 days prior to the requested start date of the annual disaster recovery test.

3.3.3 Annual disaster recovery tests will evaluate and validate that the COOP sufficiently ensures continuation of operations and the processing of TRICARE data in accordance with the TOM, Chapters 1 and 6. At a minimum, annual disaster recovery testing will include the processing of:

- TRICARE Prime enrollments in the DEERS contractor test region to demonstrate the ability to update records of enrollees and disenrollees using the Government furnished system application, DOES.
- Referrals and Non-Availability Statements (NAS)
- Preauthorizations/authorizations
- Claims
- Claims and catastrophic cap inquiries will be made against production DEERS and the Catastrophic Cap and Deductible Database (CCDD) from the relocation/recovery site. Contractors will test their ability to successfully submit claims inquiries and receive DEERS claim responses and catastrophic cap inquiries and responses. Contractors shall not perform catastrophic cap updates in the CCDD and DEERS production for test claims.
- To successfully demonstrate the ability to perform catastrophic cap updates and the creation of newborn placeholder records on DEERS, the contractor shall process a number of claims using the DEERS contractor test region.
- TED records will be created for every test claims processed during the claims processing portion of the disaster recovery test. The contractor will demonstrate the ability to process provider, institutional and non-institutional claims. These test claims will be submitted to the DHA TED benchmark area.

3.3.4 Contractors shall maintain static B2B Gateway connections or other Government approved connections at relocation/recovery sites that can be activated in the event a disaster is declared for their region.

3.3.5 In all cases, the results of the review and/or test results shall be reported to the DHA Contract Management Division within 10 days of the conclusion of the test. The contractor's report shall include if any additional testing is required or if corrective actions are required as a result of the disaster recovery test. The notice of additional testing requirements or corrective actions to be taken should be submitted along with the proposed date for retesting and the completion date for any corrective actions required. Upon completion of the retest, a report of the results of the actions taken should be provided to the CO within 10 business days of completion.

3.4 Information Security Compliance Programs

Information Security Compliance under the NIST Program is recognized by the DoD for non-DoD IS (defined as an IS that is not owned, controlled, or operated by the DoD, and is not used or operated by a contractor or other non-DoD entity exclusively on behalf of the DoD) that process Controlled Unclassified Information (CUI). Contracts governed by this manual are generally considered to be non-DoD IS.

3.4.1 Controlled Unclassified Information (CUI) and DoD Information Contractor IS

CUI is defined as "Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and Government-wide policies." DoD information is defined as "information that is provided by the DoD to a non-DoD entity, or that is collected, developed, received, transmitted, used, or stored by a non-DoD entity in support of an official DoD activity, where that information has not been cleared for public release." DoDI 8582.01. See also DoD Directive (DoDD) 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008. PII/PHI that is DoD information constitutes CUI because PII/PHI requires safeguarding or dissemination controls unless it has been cleared for public release.

3.4.2 NIST References and Related DoD Issuances

The references below support the IA requirements outlined in the following paragraphs.

- 48 CFR Parts 204, 212, and 252 as amended by 76 FR 69273 - 69282 / Vol. 78, No. 222/ November 18, 2003.
- NIST Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations"
- NIST SP 800-53A, "Guide for Assessing the Security Controls in Federal Information Systems and Organizations"
- NIST SP 800-171, "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations."
- DoDD 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008

- DoDI 8582.01, "Security of Unclassified Department of Defense (DoD) Information on Non-DoD Information Systems," June 6, 2012

- "Health Insurance Portability and Accountability Act (HIPAA), Security Standards, Final Rule," February 20, 2003

3.4.3 Compliance With Federal Programs

The NIST-based computer security program leverages a contractor's compliance with existing Federal Information Security-related measures (i.e., HIPAA, Federal Information Security Management Act (FISMA), etc.) to attest to its readiness to process CUI DoD information on non-DoD IS. This Information Security program requires participating contractors to document compliance with the security controls described in detail within the NIST SP 800-171, "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations." With respect to HIPAA Security Rule compliance, the contractor will follow the TOM, Chapter 19, Section 3, including the requirement for contractors to designate a Security Official with specified responsibilities. Those responsibilities involve compliance with HIPAA Security Rule and DHA DoD Information Security Program requirements under this section.

3.4.3.1 Risk Management

Contractors certifying compliance with the NIST-based process accept sole responsibility for the risk(s) associated with developing and maintaining its IA readiness posture.

3.4.3.2 IA Compliance Requirement

The contractor shall provide and maintain its NIST-related compliance, in order to connect to government systems.

3.4.4 NIST Certification/Recertification Procedures

3.4.4.1 Contractor Self-Certification Process

Contractors shall self-certify all IS that access, process, display, store or transmit DoD CUI. Self-certification shall be achieved, as specified in the contract. The organization shall employ Audit Review, Analysis, and Reporting through proper Integration/Scanning and Continuous Monitoring Capabilities (i.e., continuous monitoring for vulnerabilities) that identify the breadth, depth, and rigor of coverage during the security review process for submission of their self-certification documentation. Security reviews shall describe, at a high level, how the security controls and control enhancements meet those security requirements, also provide detailed, technical descriptions of the specific implementation of the controls and enhancements. The contractor shall ensure that the security controls required by the contract are implemented correctly, operating as intended, and support the security policies of the DHA.

3.4.4.2 The NIST SP 800-171, certification process, as allowed by DoDI 8582.01 and applicable contract clauses, requires compliance by contractors for the protection of DoD information provided to, contained within and/or processed by contractor IS. See Contract Data Requirements List (CDRL) for information specific to deliverables, milestones, and due dates

3.4.4.3 The contractor shall submit self-certification documents and will be notified of any identified areas that need additional information. The contractor shall respond within 10 calendar days.

3.4.5 Operation and Connectivity Decisions

3.4.5.1 The contractor shall complete and submit the NIST Certification of Compliance in accordance with the CDRL.

3.4.5.2 The contractor shall submit a written determination report for any failure to achieve and/or maintain its compliance with the NIST-based IA program.

3.4.6 Documentation

The contractor will be provided with the most current version of the NIST Checklist and Written Determination Report (WDR). If the contractor changes its compliance status with a vulnerability mitigation plan for any IA control shown on the NIST Checklist, the contractor shall submit an updated WDR statement within 10 calendar days.

3.4.7 Disposing of Electronic Media

Contractors shall follow the DoD standards, procedures and use approved products to dispose of unclassified hard drives and other electronic media, as appropriate, in accordance with DoDI 8500.1 and NIST SP 800-171.

4.0 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

The contractor shall be in compliance with the HIPAA Rules, the DoD HIPAA Issuances, the TOM, Chapter 19, Section 3, and any provisions of this manual and DoD cybersecurity guidance addressing security incident response. In particular, the contractor shall be in compliance with HIPAA breach response requirements, which are addressed in conjunction with DoD breach response requirements in the TOM, Chapter 1, Section 5.

4.1 Data Sharing Agreements (DSAs)

Contractors requiring access to PII, which includes PHI, or access to de-identified data, are subject to the DHA Privacy and Civil Liberties Office (Privacy Office) Data Sharing Program. This program requires DHA to enter into DSAs with parties outside the MHS who use or create MHS data. (DHA contracts may use the term Data Use Agreement (DUA) rather than DSA.) DSAs assure that outside parties protect MHS data in accordance with the Privacy Act and the HIPAA Rules. To apply for a DSA, the prime contractor submits a Data Sharing Agreement Application (DSAA) to the DHA Privacy Office. The contractor submits the DSAA even if a subcontractor will be the party accessing MHS data. After review and approval of the DSAA, the Privacy Office provides a DSA to the contractor for execution. The DSAA template and other DSA guidance and forms are available at the following page on the Privacy Office web site: http://health.mil/Military-Health-Topics/Privacy-and-Civil-Liberties. Primary contractors and subcontractors requiring access to or use of MHS data must also complete an Account Authorization Request Form (AARF) and have an ADP / IT-II designation. Refer to ADP/IT Category Guidance below.

4.2 Disclosure Tracking and Accounting and Other System Capabilities for Privacy Act and HIPAA Privacy Compliance

The contractor shall maintain systems (or utilize MHS systems) with the capabilities to track and report on disclosure requests, disclosure restrictions, accounting for disclosure requests, authorizations, PII/PHI amendments, Notice of Privacy Practices (NoPP) distribution management, confidential communications requests, and complaint management. Situation reports may be required to address complaints, inquiries, or unique events related to the foregoing responsibilities.

5.0 PERSONNEL SECURITY ADP/IT REQUIREMENTS

5.1 Formal Designations Required

Contractor personnel requiring access to the following must be in positions designated as ADP/IT-I (critical sensitive) or ADP/IT-II (non-critical sensitive):

- Access to a secure DoD facility;
- Access to a DoD IS or a DoD Common Access Card (CAC)-enabled network;
- Access to DEERS or the B2B Gateway.

5.2 ADP/IT Position Sensitivity Designations

5.2.1 An ADP/IT position category is a designator that indicates the level of IT access required to fulfill the responsibilities of the position, including the potential risk for an individual assigned to the position to adversely impact DoD missions or functions. The contractor's Facility Security Officer (FSO) shall use the guidance below to determine a contractor employee's specific ADP/IT level. Contractor personnel designated for assignment to an ADP/IT position shall undergo a successful background security screening before being granted access to DoD IT systems (e.g., test and/or production) and /or access to any DoD/DHA data directly extracted from any system (e.g, test and /or production) that contains sensitive data.

5.2.1.1 ADP/IT-I: Critical Sensitive Position

A position where the individual is responsible for the development and administration of MHS IS/network security programs and has the direction and control of risk analysis and/or threat assessment. The required investigation is a Single-Scope Background Investigation (SSBI) or equivalent. Responsibilities include:

5.2.1.1.1 Significant involvement in life-critical or mission-critical systems.

5.2.1.1.2 Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting severe damage to persons, properties or systems, or realizing significant personal gain.

5.2.1.1.3 Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of:

- Dollar amounts of 10 million dollars per year, or greater; or

- Lesser amounts if the activities of the individuals are not subject to technical review by higher authority in the ADP/IT-I category to ensure the integrity of the system.

5.2.1.1.4 Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring, and/or management of systems hardware and software.

5.2.1.1.5 Other positions as designated by the DHA that involve a relatively high risk for causing severe damage to persons, property or systems, or potential for realizing a significant personal gain.

5.2.1.2 ADP/IT-II: Non-Critical Sensitive Position

A position where an individual is responsible for systems design, operation, testing, maintenance, and/or monitoring that is carried out under technical review of higher authority in the ADP/IT- I category. The required investigation is a National Agency Check with Law Enforcement and Credit (NACLC) check or equivalent. Responsibilities include, but are not limited to:

5.2.1.2.1 Access to and/or processing of proprietary data, information requiring protection, or government-developed privileged information involving the award of contracts.

5.2.1.2.2 Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than 10 million dollars per year.

5.2.1.2.3 Other positions as designated by the DHA that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP/IT-I positions.

5.2.2 Employee Prescreening

5.2.2.1 The contractor shall conduct thorough reviews of information submitted on an individual's application for employment in a position that requires either an ADP/IT background check or involves access via a contractor system to data protected by either the Privacy Act of 1974, as amended, or the HHS HIPAA Privacy and Security Final Rule. For contractors working in the United States (U.S.) and the District of Columbia, this prescreening shall include reviews that:

- Verify United States citizenship;
- Verify education (degrees and certifications) required for the position in question;
- Screen for negative criminal history at all levels (federal, state, and local);
- Screen for egregious financial history; for example, where adverse actions by creditors over time indicate a pattern of financial irresponsibility or where the applicant has taken on excessive debt or is involved in multiple disputes with creditors.

5.2.2.2 For contractors working outside the United States and District of Columbia, this prescreening shall include reviews that:

- Verify United States citizenship;
- Verify education (degrees and certifications) required for the position in question;
- Screen for negative criminal history, to the maximum extent possible as permitted by local laws of the host government;
- Screen for egregious financial history, to the maximum extent possible as permitted by local laws of the host government.

5.2.2.3 The prescreening shall be conducted as part of the preemployment screening and shall be completed before the assignment of any personnel to a position requiring the aforementioned ADP/IT accesses. The prescreening may be performed by the contractor's personnel security specialists, human resource manager, hiring manager, or similar individual.

5.3 Processing Personnel Security Requirements and Granting Interim Access to DoD IS

5.3.1 Contractor requests for NACLC/SSBI types of security investigations are submitted to the federal investigating agency, Office of Personnel Management, via the electronic Questionnaires for Investigations Processing (e-QIP) system. Contractor personnel who do not have an investigation or appropriate level of investigation to obtain access to DoD/DHA IT data, systems or networks shall complete the SF 86 in e-QIP.

5.3.2 The Personnel Security Branch (PSB) may grant DHA contractor staff who are U.S. citizens, interim ADP-IT/CAC access upon confirmation of favorable results from the advance National Agency Check (NAC), FBI fingerprint check and a scheduled/open investigation at the Office of Personnel Management (OPM). PSB will notify the FSO of final adjudication determinations.

5.4 e-QIP Training and Access

5.4.1 The contractor FSO shall complete e-QIP training to access and use e-QIP.

5.4.2 The contractor FSO shall complete the e-QIP Access User Form for e-QIP user accounts to be created.

5.4.3 FSO Roles and Responsibilities

The contractor FSO shall:

- Be a U.S. citizen.
- Possess a favorably adjudicated NACLC or equivalent investigation.
- Provide list of applicants to PSB for verification of security eligibility.
- Initiate applicant's security questionnaire in e-QIP.

- Select the appropriate Agency Use Block (AUB) template in e-QIP.
- Notify the Contracting Officer's Representative (COR) by e-mail that an e-QIP request has been initiated and requires approval.
- Inform applicant to complete security questionnaire in e-QIP within 10 calendar days.
- Perform initial review of applications for required information.
- Mail two FD258 fingerprint cards to PSB.
- Verify applicant's citizenship and upload proof of citizenship document to investigation request before releasing case to PSB.
- Serve as the main point of contact (POC) for the applicant.
- Monitor the e-QIP request, which includes ensuring the applicant completes the e-QIP form within designated time period.
- Cancel or delete an e-QIP request on an applicant.
- Act as POC if DoD Central Adjudication Facility (DoD CAF) requires additional information on contractor employees.

5.5 Additional Requirements/Information

5.5.1 Background Investigation Request for ADP/IT-I

Contractors requiring an ADP/IT-I investigation for their personnel shall have their FSOs coordinate and submit a written request on contractor letterhead to the DHA COR for endorsement. The request letter shall be signed by, at a minimum, the FSO or other appropriate executive. It shall include a detailed job description which justifies the requirement for the ADP/IT-I. The justification letter shall be emailed to PSB.

5.5.2 Reinvestigation Requirements

Contractor personnel in positions designated as ADP/IT-I and ADP/IT-II have reinvestigation requirements. ADP/IT-I positions are critical sensitive and shall be re-investigated every five years. ADP/ IT-II positions are non-critical sensitive and shall be re-investigated every 10 years. The reinvestigation shall be initiated within 60 days of the closed date of the last investigation. The FSO shall track the reinvestigation requirement for contractor employees and initiate new investigations, as required above. Fingerprints are not required for re-investigations unless specifically requested. Proof of citizenship may be required, as needed.

5.5.3 Reciprocal Acceptance of Prior Investigation

An investigation is reciprocated when a new contractor employee has an existing favorably adjudicated investigation that meets the appropriate level of investigation required; and the break in service has been two years or less. The FSO shall verify prior investigation and if valid,

provide PSB with the new employee's name, Social Security Number (SSN), and Date of Birth (DOB).

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)."
- DoDI 5025.01, "DoD Issuances Program," June 6, 2014, as amended.
- DoD 5200.2-R, "Personnel Security Program," January 1987, as amended.
- U.S. Code of Federal Regulations, Title 5, Part 731, "Suitability Regulations," January 9, 2009, as amended.
- DoD Administrative Instruction 15, "Office of the Secretary of Defense Records and Information Management Program," May 3, 2013.
- Executive Order 12968, "Access to Classified Information," August 4, 1995.
- DoDM 5102.21, "Sensitive Compartmented Information Administrative Security Manual," October 2012.
- Intelligence Community Directive (ICD) 704, "Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information," October 1, 2008.
- DoDI 5200.2, "DoD Personnel Security Program," March 21, 2014.
- United States Code, Title 5, "The Privacy Act of 1974," December 31, 1974.

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 s employees hall 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, Department of Defense (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.

6.1.2 FSO Roles and Responsibilities

The contractor 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 Defense Health Agency (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).
- 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 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.

6.1.6 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.

6.1.7 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. 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.

6.1.8 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.

6.1.9 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 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
http://www.sterlingcommerce.com/solutions/products/ebi/connect/direct.html
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:

POSITION(S)	CONTENT
1 - 2	"TD"
3 - 8	YYMMDD Date of transmission
9 - 10	Contractor number
11 - 12	Sequence number of the file sent on a particular day. Ranges from 01 to 99. Reset with the first file transmission the next day.

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 -