Chapter 1 Section 1.1

General Automated Data Processing (ADP) Requirements

Revision: C-49, July 14, 2021

1.0 GENERAL

1.1 The TRICARE Systems Manual (TSM) describes how TRICARE business functions are implemented technically via system-to-system interactions and Government provided applications. The TSM also describes the technical concept of operations, including the responsibilities associated with various Information Systems (IS) including Defense Enrollment Eligibility Reporting System (DEERS), the contractor systems, and selected Direct Care (DC) IS.

1.2 The contractor shall comply with the Department of Defense (DoD) guidance regarding directed Ports, Protocols, and Services (PPS).

1.3 The contractor shall comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies. The Government will provide the contractor connectivity requirements that comply with PPS in accordance with DoD Instructions (DoDIs).

1.4 The contractor shall ensure that laptops, flash drives, and other portable electronic devices do not contain Personally Identifiable Information (PII)/Protected Health Information (PHI) unless the device is fully encrypted and accredited per National Institute of Standards and Technology (NIST) standards.

1.5 Portable electronic devices are often used to transmit reference materials and data of a general nature at meetings and conferences. The contractor shall ensure that their computer systems can accept and load all such information, regardless of the media used to transmit it. The contractor shall maintain all materials provided to the contractors at meetings, workgroups, and/or training sessions sponsored by or reimbursed by the Government in accordance with the Records Management requirements in the TRICARE Operations Manual (TOM), Chapter 9.

1.6 This chapter addresses major administrative, functional, and technical requirements related to the flow of health care related Automated Data Processing/Information Technology (ADP/IT) information between the contractor and the DoD/Defense Health Agency (DHA). The contractor shall submit TRICARE Encounter Data (TED) records as well as provider information to DHA in electronic media. This information is essential to both the accounting and statistical needs of DHA in the management of the TRICARE program and in required reports to DoD, Congress, other governmental entities, and to the public. Technical requirements for the transmission of data between the contractor and DHA are presented in this section. The requirements for submission of TED records and resubmission of records are outlined in the Chapter 2, Section 1.1, and the Government requirements related to submission and updating of provider information are outlined in Chapter 2, Section 1.2.

1.7 DoD/DHA data includes all information (e.g., test or production data) provided to the contractor for the purposes of determining eligibility, enrollment, disenrollment, capitation, fees, claims, Catastrophic Cap And Deductible (CC&D), patient health information, protected as defined by DoD 6025.18-R, or any other information for which the source is the Government. Any information received by a contractor or other functionary or system(s), whether Government owned or contractor owned, in the course of performing Government business is also DoD/DHA data. DoD/DHA data means any information, regardless of form or the media on which it may be recorded.

1.8 The ADP requirements shall incorporate standards mandated by the Health Insurance Portability and Accountability Act (HIPAA) Privacy, Security, and Breach Rules, 45 CFR Parts 160 and 164 (collectively, "HIPAA Rules"), and the DoD HIPAA Issuances identified below. Contractor compliance with the HIPAA Rules and DoD HIPAA Issuances and related privacy requirements is addressed in the TOM, Chapter 1, Section 5 and Chapter 19, Section 3 and paragraph 1.10.

1.9 TOM, Chapter 1 addresses management and quality controls specific to the accuracy and timeliness of transactions associated with ADP and financial functions. In addition to these requirements, DHA also conducts reviews of ADP and financial functions for data integrity purposes and may identify issues specific to data quality (e.g., catastrophic cap issue). Upon notification of data quality issues by DHA, the contractor shall participate in development of a resolution for the issue(s) identified as appropriate. If DHA determines corrective actions are required as a result of Government reviews and determinations, the Contracting Officer (CO) will notify the contractor of the actions to be taken by the contractor to resolve the data issues. The contractor shall take corrective actions to correct data integrity issues, resulting from contractor actions.

1.10 The references below relate to the subject matter covered in this section:

- Privacy Act of 1974.
- DoD HIPAA Issuances:
  - DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003.
  - DoD 8580.02-R, "DoD Health Information Security Regulation," July 2007.
- DoD 5200.2-R, "DoD Personnel Security Program," January 1987.
- DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007.
- DoD Directive (DoDD) 5015.2, "DoD Records Management Program," March 6, 2000.
- DoD Instruction (DoDI) 8500.01, "Cybersecurity," March 14, 2014.
- 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," August 2013.

- 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 IS).

The contractor, subcontractor(s) and other individuals with access to IS containing PII protected by the Privacy Act of 1974 and PHI under HIPAA shall meet the above requirements.

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). These meetings will:

- Review the status of system connectivity and communications.

- Identify new DEERS applications or modifications to existing applications, e.g., Government furnished web-based enrollment systems/applications.

- 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. The contractor shall 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 report any problems experienced during testing 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 shall retest the scenario to determine if the resolution is successful. The contractor shall accomplish retesting 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. The contractor shall accomplish retesting within

the agreed upon time frames. 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 numbers and emails to be used for call back purposes, notification of planned and unplanned outages and software releases. The Government will notify POCs via email in the event of an unplanned outage using the POC notification list. The contractor shall notify DHA regarding changes to the POC list.

3.0 ADP REQUIREMENTS

The contractor shall obtain and maintain 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)

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 contractor and subcontractors in order to continue operations should an actual disaster be declared for their region. The contractor shall ensure the COOP:

- Ensures the availability of the system and associated data in the event of hardware, software and/or communications failures.
- Includes the prime contractor 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.
- Includes information specific to connection to the B2B Gateway to and from the relocation/recovery site for operations in the COOP. For relocation/recovery sites, contractors shall ensure all security requirements are met and appropriate processes are followed for the B2B Gateway connectivity.
- Enables 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.
- Includes 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. See Section J of the contract for information specific to deliverables, milestones, and due dates.

3.2 Security Requirements

The contractor shall ensure security and access requirements are met in accordance with existing contract requirements for all COOP and disaster recovery activities. The Government will not grant waivers of security and access requirements for COOP or disaster recovery activities.

3.3 Annual Disaster Recovery Tests

3.3.1 The prime contractor shall coordinate annual disaster recovery testing of the COOP with its subcontractor(s) and the Government. The contractor shall ensure coordination begins no later than 90 days prior to the requested start date of the disaster recovery test. Each Prime contractor shall ensure all aspects of the COOP are tested and coordinated with all contractors responsible for the transmission of TRICARE data. Each Prime contractor shall 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 no later than 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. See Section J of the contract for information specific to deliverables, milestones, and due dates. At a minimum, annual disaster recovery testing shall include processing:

- TRICARE Prime enrollments in the DEERS contractor test region to demonstrate the ability to update records of enrollees and disenrollees using the Government furnished web-based enrollment system/application.
- Referrals.
- Preauthorizations/authorizations.
- Claims.
- Claims and catastrophic cap inquiries against production DEERS and the Catastrophic Cap and Deductible Database (CCDD) from the relocation/recovery site. Contractors shall 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.
- 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. The contractor shall create TED records for every test claim processed during the claims processing portion of the disaster recovery test. The contractor shall demonstrate the ability to process provider, institutional and non-institutional claims. The contractor shall submit these test claims to the DHA TED landing area.

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

3.3.5 In all cases, the contractor shall report results of the review and/or test results to the DHA Managed Care Contracting Division (MC-CD) within 10 days of test conclusion. 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 contractor shall submit notice of additional testing requirements or corrective actions to be taken along with the proposed date for retesting and the completion date for any corrective actions required. Upon completion of the retest, the contractor shall provide a report of the results of the actions taken to the MC-CD within 10 business days of completion. See Section J of the contract for information specific to deliverables, milestones, and due dates.

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 processes 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

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 / Monday, November 18, 2013.
- 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 shall 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 as required by the contract, in order to connect to Government systems.

3.4.4 NIST Certification/Recertification Procedures

3.4.4.1 Contractor Self-Certification Process

The contractor shall self-certify all IS that access, process, reproduce, modify, perform, store, display, release, disclose, or disseminate CUI. The contractor shall achieve self-certification, as specified in the contract. The contractor 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. The contractor shall ensure security reviews describe, at a high level, how the security controls and control enhancements meet those security requirements, and 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. The following process applies to the NIST-based Information Security certification process. See Section J of the contract for information specific to deliverables, milestones, and due dates.

3.4.4.3 The contractor shall submit self-certification documents and the Government will notify the contractor regarding any identified areas that need additional information. The contractor shall respond within 10 days.

3.4.5 Operation and Connectivity Decisions

3.4.5.1 The contractor shall complete and submit the NIST Certificate of Compliance in accordance with Section J of the contract for information specific to deliverables.

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 Government will provide the contractor with the most current version of the NIST Checklist and Written Determination Report (WDR) within 10 days of contract award. 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 days.

3.4.7 Disposing of Electronic Media

The contractor 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 DoDD 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 Defense Privacy and Civil Liberties Office (DPCLO) (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 shall submit a Data Sharing Agreement Application (DSAA) to the DHA DPCLO. 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 shall 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 use 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. The contractor shall submit situation reports as necessary 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 shall be in ADP/IT-I (critical sensitive) or ADP/IT-II (non-critical sensitive) designated positions:

- 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 includes access to DoD information systems. It 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. The contractor shall ensure its personnel designated for assignment to a ADP/IT position undergo a successful background security screening before being granted access to DoD Information Technology (IT) systems and/or any DoD/Defense Health Agency (DHA) data directly extracted from those contained on 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 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, 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 Designated Approving Authority (DAA) 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 ADT/IT- I category. The required investigation is a National Agency Check with Law Enforcement and Credit 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 DAA 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 investigation 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 U.S. 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 U.S. and District of Columbia, 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 contractor shall conduct prescreening as part of the pre-employment screening, and shall complete the prescreening before the assigning of any personnel to a position requiring the aforementioned ADP/IT accesses. The pre-screening shall 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 The contractor shall submit requests for a NACLC/SSBI type of security investigation 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 contractors that are U.S. citizens interim ADP-IT/CAC access upon confirmation of favorable results from the advance NAC, FBI fingerprint check and a scheduled/open investigation at OPM.

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 email that an e-QIP request has been initiated and requires their approval.
- Inform applicant to complete security questionnaire in e-QIP within 10 calendars days.
- Perform initial review of applications for required information.

- Capture and transmit e-fingerprints to OPM via Secured Web Fingerprint Transmission (SWFT) or 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 in designated time period.
- Cancel or delete an e-QIP request on an applicant.
- Act as POC if DoD Central Adjudication Facility (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 company 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 a company assigned POC in 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 contractor shall initiate reinvestigation 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.

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 is two years or less. The FSO shall verify prior investigation and if valid, provide PSB 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. PSB will notify the FSO regarding the required information and a due date. If the contractor does not provide the required information by the due date, the Government may reject the investigation or return it. The FSOs 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. The contractor shall email notification and include the employee's name and termination date. The contractor shall immediately notify PSB if they move an employee to another one of its DHA contracts, especially when an employee is being moved from an unclassified contract to a classified contract.

5.5.5.2 PSB will notify FSOs 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 contractor shall return the return receipt letter (included with the denial letter from PSB) to PSB within one week after receipt of the letter to show compliance with terminating 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. The gaining contractor shall notify PSB when this type of transfer occurs. The notification shall contain the employee's name and the effective date of transfer.

5.5.7 Electronic Fingerprint Capture and Submission

The contractor shall capture e-fingerprints and transmit via SWFT as it improves processing time and securely transmits fingerprints. The contractor and its subcontractors with access to DoD IS containing information protected by the Privacy Act of 1974 and PHI under HIPAA, shall meet these requirements.

5.5.8 Foreign Nationals

The requirements above shall be met by U.S. citizens who have access to DoD IS containing information protected by the Privacy Act of 1974 and PHI under HIPAA. The contractor shall ensure the required investigation is completed and favorably adjudicated prior to authorizing ADP/IT access to DoD system/networks.

5.5.9 Notification and Mailing

The contractor shall use the following information to contact the PSB. The contractor shall handle sensitive information according to applicable laws and DoD policies related to privacy and confidentiality. The contractor shall transmit personally identifiable information or protected health information via encrypted email or the OPM secure portal.

Mailing Address:

Defense Health Agency
ATTN: Personnel Security Branch
7700 Arlington Blvd., Suite 5101

Falls Church, VA 22042-5101

e-QIP Help Desk: (703) 681-6508
Email address: dhapsb@mail.mil

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, "DoD Issuances Program," June 6, 2014, as amended.
- DoDD 52002.2-R, "Personnel Security Program," January 1987, as amended, http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf.
- FIPS Publication 140-2, Security Requirements for Cryptographic Modules, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.
- 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.
- DoDD 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.
- United States Code, Title 5, "The Privacy Act of 1974," December 31, 1974.

6.0 PUBLIC KEY INFRASTRUCTURE (PKI)

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 is 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. To meet this requirement, contractor employees shall obtain Government-issued CACs. PIV compliant credentials are required for access to DoD systems, networks and data. The Government will not grant alternate sign on access. The contractor shall use encryption and digital signatures for electronically transmitted information 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.

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

The Government will issue, reissue, or replace CACs with a blank email certificate unless the CAC holder already has a DoD approved email address. Instructions for requesting an approved email address are available in paragraph 6.1.1.3.3. Without an approved Government email address (and the accompanying DoD email 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 email certificate authentication. CAC capabilities that do not require a DoD approved email certificate for authentication will still function. If a CAC owner requires a DoD approved email certificate to perform their duties, the DHA's DoD approved email is Defense Enterprise Email (DEE). Not all contractors require DoD approved email 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 Email Address Certificates on CACs

6.1.1.3.2 CAC owners need a DoD approved email 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 DoD approved email address certificate assigned and the email address certificate will remain blank. Some current CAC users may already have another type of email certificate that complies with DoD requirements. If a contractor requires the capabilities afforded by a DoD approved email certificate on their CAC, the contractor shall obtain a DEE account, as described below. The DEE account provides the CAC holder with the necessary DoD approved email certificates for the CAC. It also creates an email inbox that allows the user to send/receive encrypted emails and send/receive Government correspondence, among other capabilities. Once a CAC holder obtains their DEE account, the holder may access the account via Outlook Web Access (OWA) at https://web.mail.mil.

6.1.1.3.3 Upon request from the Contracting Officer's Representative/Program Manager (COR/PM), the contractor FSO shall email 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 to the

COR. Upon receipt, the COR/PM will forward the information to GSC DHA.ITCallCenter@mail.mil and request DEE accounts 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 along with instructions on how to create or update their DEERS/Real-Time Automated Personnel Identification Systems (RAPIDS) Online profiles as described below.

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

- Update the email 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 Email.
  - Update the DoD approved email 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, the initial and/or renewal CAC.
- Submit 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 email to dha.ncr.security.mbx.personnel-security-tass@mail.mil.

6.1.2.2 Obtaining Email Address Certificate

The FSO shall:

- Assist the CAC owner with obtaining a DoD approved email address (and the accompanying email 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, personal type codes (Civilian, Military, Contractor) and DoD ID Number, for those requiring an email 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 applicant's CAC.
- Return CACs 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. When possible, the ID card shall be electronically authenticated in lieu of photographing the card.

6.1.3.2 The contractor shall not amend, modify, or overprint ID cards by any means. The contractor shall not place stickers or other adhesive materials on either side of an ID card. The contractor shall not punch holes into ID cards, except when a CAC has been requested by the next of kin for an individual who has perished in the line of duty. The contractor shall ensure the status of the CAC is revoked in DEERS, the certificates are revoked, and a hole is punched through the integrated circuit chip before it is released to the next of kin.

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 CAC at all times while affiliated with the DoD.

6.1.3.5 Multiple Cards

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

6.1.3.6 Renewal and Reissuance

The applicant for CAC renewal or reissuance shall surrender the current CAC card that is up for renewal. The individual shall renew their CAC 90 days prior to the CAC expiring.

6.1.3.7 Replacement

The applicant shall provide a letter from the local security office confirming the CAC has been reported lost, stolen confiscated or destroyed, and 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 and returned to TASS-CACB when the card has expired, is damaged, compromised, when the applicant is no longer affiliated with the DoD contractor or no longer meets the eligibility requirements for the card.

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 individual shall get the PIN 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 shall not be done remotely. The Government will provide CPR software licenses; the contractor shall provide all hardware for the workstation (PC, Card Readers, Fingerprint capture device). The contractor shall not use the CPR workstation for other applications, as the Government has not tested the CPR software for compatibility. The contractor shall ensure the CPR software is installed on the desktop and not 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 Systems Requirements for CAC Authentication

The contractor shall procure, install, and maintain desktop level CAC readers and middleware. The contractor shall ensure the middleware software runs on the desktop and not be run from the LAN. For CAC and CAC reader technical specifications go to 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 shall 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. The contractor shall not allow CACs, PINs, and other access code sharing.

6.1.7 The contractor shall provide to the Government the locations and approximate number of contractor personnel by site who require CAC issuance 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) Medical Community of Interest (MedCOI) B2B Gateway

7.1.1 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 shall include acquiring and maintaining the circuit used to connect to the B2B Gateway and the acquisition of a Virtual Private Network (VPN) device maintenance agreement and license compatible with the MHS VPN device. The list of compatible devices are detailed in the DHA B2B/MedCOI Gateway questionnaire.

7.1.2 The contractors shall submit a completed current version of the DHA B2B/MedCOI Gateway questionnaire to their Government sponsor or Government Program Office within 10 days after new requirements have been provided to the contractor. The contractor shall provide information specific to their connectivity requirements, proposed path for the connection and last mile diagram. The contractor shall submit the completed questionnaire directly to the DHA B2B office or through the contractor's Government Program Office/sponsor for review and scheduling of an initial technical specifications meeting.

7.2 Contractor Provided IT Infrastructure

7.2.1 The contractor shall ensure its platforms support HyperText Transfer (Transport) Protocol (HTTP), HyperText Transfer (Transport) Protocol Secure (HTTPS), web-derived Java Applets, and Secure File Transfer Protocols (SFTPs) (e.g., STFP, Secure Socket Layer (SSL)/Transport Layer Security (TLS)), 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. The contractor shall not use dial-up ISP connections. The contractor shall ensure all IP addresses are publicly routable. The contractor shall not use Network Address Translation (NAT) for private address space.

7.2.4 The contractor shall maintain a valid maintenance contract and pertinent licenses for all devices connecting to the MHS B2B Gateway.

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 shall submit the most current version of DD Form 2875 in accordance with CO guidance. The contractor shall complete a DD Form 2875 for each contractor employee who will access any system and/or application on a DoD network. The contractor shall ensure the DD Form 2875 clearly specifies the system and/or application name and justification for access to that system and/or application.

7.3.2 The contractor shall submit the completed DD Form 2875 to the DHA DPCLO for verification of ADP Designation. The DHA DPCLO will verify that the contractor employee has either a complete appropriate background investigation or one requested from OPM. DHA DPCLO will verify the background investigation request and scheduled investigation with OPM prior to approving access.

7.3.3 The DHA DPCLO will forward the DD Form 2875 to I&OD for processing; I&OD will forward DD Form 2875s to DHA. DHA will notify the user of the ID and password via secure/encrypted email 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 DPCLO with a report of the findings of their review by the 10th day of each month following the review. Details for reporting are identified in DD Form 1423, Contract Data Requirements List (CDRL), located in Section J of the applicable contract.

7.4 MHS Systems Telecommunications

7.4.1 The contractor shall ensure primary communication links are via encrypted tunnels (i.e., Secure Internet Protocol (IPSEC), GetVPN, or SSL) 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 DHA 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, the contractor shall procure an auxiliary VPN device for contractor locations and configure devices for operation to minimize any downtime associated with problems of the primary VPN.

7.4.4 The contractors send devices to the MHS VPN management authority (e.g., DHA) postage paid and include prepaid return shipping arrangements for the devices(s).

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

7.4.6 The contractor shall maintain and repair contractor procured VPN equipment. The Government will troubleshoot of VPN equipment.

7.5 Establishment of Telecommunications

7.5.1 The contractor shall establish telecommunications with the MHS in coordination with DHA. The contractor shall identify their requirement(s) for the establishment of telecommunications with the MHS, DMDC or other Government entities.

7.5.2 The DHA/MedCOI B2B Gateway Questionnaire (provided by DHA) identifies the required telecommunication infrastructure between the contractor and the MHS systems. This includes all Wide Area Network (WAN), LAN, VPN, Web DMZ, and B2B Gateway access requirements. The contractor shall complete their applicable portion of the questionnaire and shall return it 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 review and process the questionnaire when it is accepted.

7.5.3 DHA will coordinate any requirements for additional information with the POC and schedule any meetings required to review the Questionnaire. Upon approval of the Questionnaire, DHA will coordinate a testing meeting with appropriate stakeholders. 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 DHA with a copy of the approved and signed B2B Questionnaire for all telecommunication efforts upon request.

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 Market/Military Treatment Facilities (MTFs) and Base/Post/Camp communication personnel. The Government will furnish these connections.

7.6.2 Contractors located on military installations that require direct connections to their networks shall provide an isolated IT infrastructure. The contractor shall coordinate with the Base/Post/Camp communications personnel and the Market/MTF to get approval for a contractor procured circuit prior to installation 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. The contractor shall ensure all network traffic is via Transmission Control Protocol/Internet Protocol (TCP/IP) using ports and protocols in accordance with current Uniformed 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 San Antonio, TX; and operated by the DISA Defense Enterprise Computing Center (DECC), Detachment San Antonio, TX.

Note: The location of the primary site may be changed. The Government will advise the contractor if the primary site changes.

7.7.2 General

The common means of administrative communication between Government representatives and the contractor is via telephone and email. DHA may approve an alternate method. At the start-up planning meeting, each contractor on the telecommunication network shall provide DHA the name, address, and telephone number of the technical POC and update the information when changes occur. The contractor shall also provide a separate computer center (Help Desk) number to DHA for the DHA computer operator to use for data transmission problem resolution.

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 The contractor shall use file transfer software 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 may 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 The contractor shall provide TCP/IP communications software incorporating the TN3270 emulation, for ports and protocol support.

7.7.3.1.3 The contractor shall not transmit more than any combination of 400,000 records at one time.

7.7.3.1.4 "As Required" Transfers

The contractor shall coordinate and execute ad hoc movement of data files through 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. The contractor shall obtain destination file names 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 The contractor shall ensure all files received by and sent from the DHA data processing site comply with the following standards 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

7.7.3.1.6.1 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.

7.7.3.1.6.2 Alternate Transmission

Should the contractor not be able to transmit their files through the normal operating means, the contractor shall notify DHA 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 described in the TOM.

7.9 DHA/TRICARE Duplicate Claims System (DCS)

The DCS is a web application accessible via Microsoft Internet Explorer (MSIE) version 6.0, 7.0 or as directed by the Government. The contractor shall provide internal connectivity to the public Internet and shall supply all systems and operating system software needed internally to support the DCS. (See Chapter 4 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 DHA private care contractors. DHA 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 Defense Health Agency (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

The contractor shall transmit Army, Air Force, Navy, Marines, and Space Force pay allotment data to DFAS via the B2B Gateway using 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 anything already submitted for B2B access.

7.10.1.2 USCG and PHS

The contractor shall transmit USCG and PHS payroll allotment data via the SilkWeb (a SFTP) and Titan web application (see instructions in Addendum A). All security and data handling requirements in this Chapter remain in effect. In addition, the 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 or TRICARE Select 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 POCs to the DFAS/USCG/PHS for testing, system and ongoing business requirements. The contractor shall maintain POC information and include: name, title, contractor name, address, electronic mail address and telephone number. The contractor shall provide updated information 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. The contractor shall only include new allotments and stops and/or changes for subsequent files.

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

7.10.2.5 The contractor shall email notification to DFAS/USCG/PHS regarding 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 A. The CO will notify the contractor regarding changes to the file layout.

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

7.10.4 Data Transmission Schedule

7.10.4.1 The contractor (or their designated subcontractor) shall transmit data 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 the contractor shall transmit all data 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. In the accompanying email, the contractor shall indicate the file does not contain 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 documents 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 file submission.

- END -