

GENERAL ADP REQUIREMENTS

1.0. GENERAL

1.1. The TRICARE Systems Manual defines the contractor's responsibilities related to automated processing of health care information and transmission of relevant data between the contractor and **TRICARE Management Activity (TMA)**. It covers three major categories of information flowing among the contractor and **TMA/Defense Enrollment Eligibility Reporting System (DEERS)**: health care coverage information; provider information; and pricing information. For each of these categories it presents specifics of submission, record and data element specifications, editing requirements, and TMA reporting of detected errors to the contractor.

1.2. This chapter addresses major **administrative**, functional and technical requirements related to the flow of health care related **Automated Data Processing (ADP)** information between the contractor and TMA. TRICARE Encounter Data (TED) records as well as provider and pricing information **shall** be submitted to TMA in electronic media. This information is essential to both the accounting and statistical needs of TMA in management of the TRICARE program and in required reports to Department of Defense, Congress, other governmental entities, and to the public. Technical requirements for the transmission of data between the contractor and TMA are presented in this section. The requirements for submission of TRICARE Encounter Data records and resubmission of records are outlined in **Chapter 2, Section 1.1**, the TMA requirements related to submission and updating of provider information **are** outlined in **Chapter 2, Section 1.2** and the TMA requirements related to submission and updating of pricing information **are** outlined in **Chapter 2, Section 1.3**.

1.3. The ADP requirements **shall** incorporate the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** mandated standards where required.

2.0. ADP REQUIREMENTS

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

2.1. Continuity of Operations **Plan (COOP)**

2.1.1. The contractor shall develop a plan to ensure the **continuous operation** of their **information technologies (IT)** systems and data support of TRICARE. The COOP shall ensure the availability of the system and associated data in the event of hardware, software and/or communications failures. The contractor shall develop a COOP that will enable compliance

with all processing standards as defined in the TRICARE Operations Manual, [Chapter 1, Section 3](#).

2.1.2. The contractor **shall** conduct a test of the backup system within the first quarter of the initial health care delivery period and **shall** continue to assure backup capabilities by testing or reviewing the availability and capability of the backup ADP system to process the TRICARE data and produce the expected results. The contractor's testing of the backup system **shall** be done at least once a year.

2.1.3. The test in the first quarter and the annual test **shall** include a representative sampling of at least four hundred (400) of the various health care records routinely processed by the contractor. If the test does not produce results which are equal to those achieved on the contractor's primary system, the contractor shall take immediate steps, and within ninety (90) days reestablish a backup ADP system acceptable to TMA. In all cases, the results of the review and/or test results **shall** be reported to **the TMA, Contract Management Division** within fifteen (15) days of conclusion of the review or test.

2.2. Security

2.2.1. All contractors shall comply with DoD and MHS security requirements.

2.2.2. The contractor has the responsibility to ensure that TRICARE program records in its custody, whether in machine readable form or hardcopy, are protected from unlawful disclosure, fraud or embezzlement. The Privacy Act of 1974, HIPAA Privacy Rule, and all DoD Privacy requirements are applicable to production, test, and distribution of hardcopy reports, to labeling and mailing of magnetic tapes, to restrictions of online access to data files, and to destruction of reports and magnetic tapes. These records **shall** be protected from malicious or inadvertent destruction, and also from loss due to natural disasters.

2.2.3. TRICARE Operations Manual, [Chapter 1, Section 5](#) outlines specific statutory requirements for control and/or release of information. The contractor, in processing TRICARE data, develops and maintains information files which fall within requirements of these laws. Control of access, either physically or electronically, to the contractor's TRICARE program software, operational data files, documentation libraries, and off-site storage areas **shall** be limited to those persons with a legitimate need to access and use the information. All factors discussed above **shall** form a basis for the contractor's security plan.

2.3. Information Assurance Background

OMB Circular A-130, "Management of Federal Information Resources," requires Certification and Accreditation (C&A) of all Federal Automated Information Systems (AISs)/networks every three years at a minimum or as changes that require re-accreditation occur. Further, the accrediting agency may request annual systems reviews. This C&A requirement ensures the effective safeguarding of sensitive but unclassified (SBU) information against unauthorized modification, disclosure, destruction, and denial of service.

Certification is the comprehensive evaluation of the technical and non-technical security features and countermeasures of **AISs/networks**. Certification is conducted in

support of the accreditation process, to establish the extent that a particular system design and implementation meet a set of specified security requirements. Certification also determines the appropriate level of protection for the AIS/network. Accreditation is the formal approval by the Government to:

- Operate the AIS/network in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
- Operate within the given operational environment with stated interconnections.
- Operate with appropriate level-of-protection for the specified period.

The Military Health System (MHS) performs C&A of its AISs/networks in accordance with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)." The objective of the DITSCAP is to maintain a standardized approach to security C&A for AISs/networks. The process is designed to protect and secure those entities that comprise the DoD Global Information Grid (GIG). The process is comprehensive and considers the AIS/network mission, environment, and architecture while assessing the impact of operation of that AIS/network on the GIG.

One key aspect of the C&A process checks is whether appropriate actions have been initiated to ensure compliance with DoD 5200.2-R, "Personnel Security Program," which requires all contractors who manage, design, develop, operate, or access DoD AISs/networks to undergo an appropriate background investigation and security awareness training before access is granted to a DoD AIS/network. In those cases where controlled unclassified information (e.g., critical technologies and Privacy Act data) is maintained in Contractor Owned Contractor Operated (COCO) AISs/networks that have no interconnection with DoD AISs/networks, other safeguards (e.g., non-disclosure agreements, training) authorized in accordance with other applicable guidance may be used in lieu of background investigations to mitigate the risks associated with the loss/misuse or unauthorized access to or modification of controlled unclassified information. Adherence to these requirements provides protection of DoD AISs/networks, information technology (IT) resources, and DoD SBU information and is an absolute priority in order to provide world-class health support to the warfighter during peacetime and wartime.

3.0. TECHNICAL SERVICES REQUIRED

3.1. Information Assurance Task Description

The contractor shall ensure DITSCAP documentation availability and MHS acceptability, assist the government's MHS Information Assurance (IA) C&A Team during all phases of the C&A process, and implement processes to provide a C2 level of security. The contractor shall ensure appropriate background investigations are initiated and security awareness training for their personnel is completed before access to DoD AISs/networks or DoD SBU information is granted. The contractor shall coordinate all activities associated with this task, with the MHS IA Program Office, the Contracting Officer's Technical Representative, and the DITSCAP Designated Approving Authority (DAA) when appropriate, before any action is taken.

3.2. Scope Of Work

3.2.1. DITSCAP Requirements

The C&A requirements apply to all DoD AISs/networks and COCO AISs/networks that interconnect to DoD AISs/networks. The only exception is when the COCO AIS/network does not interconnect with a DoD AIS/network. In this case the DITSCAP requirements do not apply, and other safeguards may be used. When completing the DITSCAP, the contractor shall prepare all required documents and modify those documents as necessary to incorporate any Certification Authority (CA) recommendations. Contractors shall be required to mitigate all vulnerabilities identified for correction during the risk assessment process.

The contractor shall work with the MHS IA C&A Team during the DITSCAP by providing technical (systems security) information and AIS/network access as needed to thoroughly execute the C&A mission. In addition, the contractor shall implement organizational processes necessary to provide C2 level of security for DoD and COCO AIS's/network interconnectivity. C&A activities shall be coordinated with the MHS IA Program Office. Further, the contractor shall prepare, submit, and maintain copies of all required documentation to ensure DITSCAP compliance.

3.2.2. ADP/IT Requirements

The ADP/IT requirements apply to those individuals who manage, design, develop, operate, or access DoD AISs/networks. Such individuals shall undergo an appropriate background investigation and security awareness training before access is granted to a DoD AIS/network. This also applies to personnel accessing COCO AISs/networks with interconnection to DoD AISs/networks. COCO AISs/networks with access to DoD SBU information that have no interconnection to DoD AISs/networks may use alternative safeguards in lieu of background checks.

In addition to initial security awareness training, all contractors shall implement and document annual security awareness training for personnel working with DoD SBU information. Furthermore, the contractor shall prepare, submit, and maintain copies of all required documentation for the ADP/IT background investigation requirements.

3.3. Statement Of Work

3.3.1. DITSCAP

The contractor shall acquire/develop and maintain DITSCAP documentation to ensure both initial and continued DITSCAP compliance for all contractor AISs/networks **interconnected with DoD AISs/networks**. In addition, the contractor shall modify the DITSCAP documents as required to address system and/or procedural changes. The contractor shall assist the MHS IA C&A Team during all phases of the C&A process by providing documentation in accordance with the MHS IA C&A schedule. Upon contract award, the contractor **shall** be prepared to execute the DITSCAP process by providing required documentation necessary to receive an Approval to Operate (ATO), and by making the contractor's AIS/networks available for testing. Contractors **shall** be required to mitigate

all vulnerabilities identified for correction during the risk assessment process. These requirements shall be met before fielding the system, and before interconnecting with any DoD AIS or network is authorized. The only exception is when the COCO AIS/network does not interconnect with a DoD AIS or network, then DITSCAP requirements do not apply. However, the contractor shall put in place processes that provide and ensure security protection for COCO AISs/networks that process DoD SBU information.

3.3.2. MHS IA C&A Team

The contractor shall assist the government's MHS IA C&A Team during all phases of the DITSCAP. The MHS IA C&A Team shall require systems access in order to facilitate the script testing and automated scanning necessary to qualify the contractor's AISs/networks for C&A. All scans and testing shall be scheduled and conducted in coordination with the MHS IA Program Office, the Contractor, and the Contracting Officer's Technical Representative.

3.3.3. C2 Level Requirements

DoD requires all contractors who design, develop, manage, operate, or access DoD AISs/networks or COCO AISs/networks interconnected with DoD AISs/networks to ensure that a C2 level of trust is achieved and maintained. The contractor shall:

- Obtain DITSCAP documents published by DoD. These documents can be obtained from: http://www.tricare.osd.mil/tmis_new/pcp.htm.
- Comply with DITSCAP requirements.
- Ensure contractor personnel receive initial and annual security awareness training.
- Comply with the requirements for Information Assurance Vulnerability Management (IAVM) program. Contractors can sign-up to a List Server for IAVA notifications at <http://www.cert.mil> or <http://www.cert.org>.
- Report out-of-the-ordinary events such as intrusion, denials of service, malicious logic attacks, and probes to a Computer Emergency Response Team (CERT). Contractors shall have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of operations. These incidents shall be reported to the CERT immediately.
- Ensure adequate protection is provided to safeguard all contractor AISs/networks that process DoD SBU information.

3.3.4. ADP/IT Requirements

The contractor shall initiate and document all activities necessary to establish any ADP/IT background investigations for each contractor employee required to support the ADP/IT level of the positions held. This ADP/IT process establishes the level of access to be afforded to every contractor employee using DoD AISs and networks, as well as individuals accessing COCO systems connected to DoD AISs/networks. In cases where controlled unclassified information is maintained in COCO AISs/networks that have no interconnection with DoD AISs/networks, other appropriate safeguards (e.g., contractor

hiring process for trustworthiness, non-disclosure agreements, training) are authorized in lieu of background investigations.

3.3.4.1. ADP/IT Position Categories

In establishing the categories of positions, a combination of factors may affect the determination, permitting placement in higher or lower categories based on the agency's judgment as to the unique characteristics of the system or the safeguards protecting the system. A level of trustworthiness shall be established before granting personnel access to DoD SBU information, DoD AISs/networks or contractor AISs/networks with DoD interconnection, to include:

- ADP/IT-III - Non-sensitive Position. All positions other than ADP/IT-I and II involved in computer activities.
- ADP/IT-II - Non-critical-Sensitive Position. Those positions in which the individual is responsible for the direction, planning, design, operation, or maintenance of a computer system, has privileged access to AISs/networks, and whose work is technically reviewed by a higher authority of the ADP/IT-I category to insure the integrity of the system.
- ADP/IT-I - Critical Sensitive Position. Those positions in which the individual is responsible for the planning, direction, and implementation of a computer security program and has privileged access to AISs/networks; major responsibility for the direction, planning and design of a computer system, including the hardware and software; or, can access a system during the operation or maintenance in such a way, and with a relatively high risk for causing grave damage, or realize a significant personal gain.

Each contractor shall be required to complete and submit for appropriate personnel the Standard Form 86, "Questionnaire for National Security Positions," fingerprint forms, and such other documentation as may be required by the Office of Personnel Management (OPM) to open and complete investigations. Following submission, an interim (temporary) clearance may be provided while this investigation is ongoing. Forms and guidance can be found at <http://www.opm.gov/extra/investigate>. NOTE: The appropriate billing code that must be entered on the Standard Form 86 (referred to in [Chapter 1, Addendum A](#) (Appendix 6 of DoD 5200.2-R, Section 6.8.4.)), will be provided following contract award.

Investigations appropriate for position sensitivity designations are:

ADP/IT-III - National Agency Check (NAC)

- Records check of designated Federal Government agencies (i.e., Federal Bureau of Investigation, Central Intelligence Agency, Immigration and Naturalization Service) that maintain records relevant to making a personnel security determination. The NAC is an integral part of all investigations.

ADP/IT-II - National Agency Check with Law and Credit (NACLC) investigation

- Includes an NAC
- Financial Review covering the last seven years
- Confirmation of date and place of birth
- Law enforcement agency check

ADP/IT-I - Single Scope Background Investigation (SSBI)

- NAC for the subject
- NACLC for the subject
- NAC for the spouse or cohabitant
- Verification of U.S. citizenship
- Verification of claimed education
- Employment: verification of the past seven years
- Verification of all prior Federal and military service

Interim Assignment: For U.S. citizens, including temporary, intermittent, volunteers, and seasonal personnel, efforts shall be taken to approve ADP/IT-I, ADP/IT-II, and ADP/IT-III positions on an interim basis prior to a final adjudication of the required personnel security investigation, only after the conditions specified below have been met.

ADP/IT-III:

- A favorable review of local personnel (e.g., human resources records), base/military, medical, and other security records as appropriate
- Initiation of a NAC and favorable review of SF86 by the Government sponsor's security manager/official.

ADP/IT-II:

- A favorable review of local personnel (e.g., human resources records), base/military, medical, and other security records as appropriate
- Initiation of a NACLC and favorable review of SF86 by Government sponsor's security manager/official.

ADP/IT-I:

- Favorable completion of the NAC for the subject
- Initiation of an SSBI and favorable review of SF86 by Government sponsor's security manager/official

For DoD contractor personnel, any interim approval shall be made by the Government sponsor's security manager/official or designee.

3.3.5. Non-U.S. Citizens

Non-U.S. citizen contractor employees shall not be assigned to ADP/IT-I positions.

Non-U.S. citizen contractor employees assigned to ADP/IT-II or ADP/IT-III positions shall have a completed investigation and favorable adjudication prior to access. Interim access is not authorized.

3.3.6. Security Documentation

DITSCAP documentation shall be developed, maintained, and provided by the contractor to achieve accreditation. During the period of performance, the contractor shall modify DITSCAP documents to incorporate the comments of the CA and/or to account for all security system changes. All AISs/networks that interconnect with DoD AISs/networks shall require security C&A in accordance with DoD DITSCAP (DoDI 5200.40). The contractor shall produce and finalize all DITSCAP documents, including preparation of a System Security Authorization Agreement (SSAA) and required appendices (Deliverable #1 of DITSCAP). The SSAA is the defining document that supports the DITSCAP. The SSAA is a living document that is used throughout the entire DITSCAP to guide actions, document decisions, specify C2 requirements, identify potential solutions to risks and vulnerabilities identified, and maintain operational security. The primary objectives of the SSAA are to document:

- The formal written agreement among the DAA, CA, User Representative, and Program Manager.
- All requirements necessary for accreditation and how requirements are met.
- All security criteria required throughout the AIS/network life cycle.
- The DITSCAP Plan (e.g., a list of activities and associated timelines for achieving C&A).

The SSAA consolidates the system and security documentation into one master document. This eliminates redundancy and potential confusion. When feasible, the SSAA can be tailored to incorporate existing documents as appendices or by reference to the pertinent document.

The required core chapters within the body of the SSAA shall include the following:

- Chapter 1 - Mission Description and System Identification
- Chapter 2 - Environment Description
- Chapter 3 - System Architectural Description
- Chapter 4 - System Security Requirements
- Chapter 5 - Organizations and Resources
- Chapter 6 - DITSCAP Plan

Additionally, the contractor shall provide the following documents as SSAA appendices:

- Acronym List
- Glossary of Terms
- Reference List
- System Concept of Operations
- Information System Security Policy
- Requirements Traceability Matrix
- Certification Test and Evaluation Plan
- Security Test and Evaluation (ST&E) Procedures
- Security Features Users Guide (SFUG)
- Trusted Facility Manual (TFM)
- Security Design Document (SDD)
- Configuration Management Plan
- Installation Guide
- Rules of Behavior
- Incident Response Plan
- Contingency Plans
- Personnel and Technical Security Controls
- MOA's for System Interfaces
- Security Awareness Training Program

ADP/IT personnel security documentation shall be initiated, maintained, and documented by the contractor. This documentation shall be made available for review by the Contracting Officer's Representative (COR). The only exception is when a COCO AIS/network does not interconnect with a DoD AIS or network. In this case, background investigations for contractor personnel are not required and other safeguards may be used.

A level of trustworthiness shall be established before granting access to DoD SBU information contained in DoD AISs/networks or COCO AISs/networks interconnected with DoD AISs/networks. In those instances, the contractor shall:

- Initiate, maintain, and document minimum personnel security investigations appropriate to the individual's responsibilities.
- Immediately report to the appropriate government representative if any contractor employee filling a sensitive position receives an unfavorable National Agency Check (NAC) adjudication, or if information that would result in an unfavorable NAC becomes known.
- If at any time, an individual receives an unfavorable NAC adjudication, or if directed by the appropriate government representative for security reasons, that individual will be immediately denied access.
- Ensure all contractor personnel receive initial and annual security awareness training.

All contractor personnel in positions requiring access to DoD AISs/networks or COCO AISs/networks interconnected with DoD AISs/networks must be designated as

ADP/IT-III, ADP/IT-II, or ADP/IT-I where their duties meet the criteria of these position sensitivity designations as described in DoD 5200.2-R. See Chapter 1, Addendum A.

3.4. Public Key Infrastructure (PKI)

The DoD has initiated a Public Key Infrastructure Policy to enhance the identification and authentication of users and system within DoD. The PKI program is in its initial stage and is evolving. The following paragraphs provide current DoD PKI requirements. Additional guidance as it applies to this contract will be provided as the policy and implementation guidance is finalized within DoD.

The contractor is required to obtain PKI certificates for individuals that will be directly accessing any of the following DoD client/server or web applications:

- The Defense Online Enrollment System (DOES) - [DEERS client/server application]
- The General Inquiry of DEERS (GIQD) application - [DEERS web application]
- The TRICARE Duplicate Claims System - [TMA web application]

Contractor personnel that access these systems from a .mil domain will be eligible to receive their certificates from the Government. PKI certificates for contractor personnel that access the above listed systems from non-.mil domains may be purchased through DoD approved External Certification Authorities (ECAs). For additional guidance for obtaining External Certificate Authority user certificates, the following URL is provided: <http://www.disa.mil/infosec/pkieca/documents.html>.

Additionally the contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers involved in the following system-to-system or host-to-host Secure Socket Layer (SSL) interfaces:

- Contractor systems for claims eligibility inquiries and responses and DEERS
- Contractor systems and the TRICARE Encounter Data (TED) Processing Center

3.5. For additional guidance for obtaining External Certificate Authority server certificates, the registration procedure requirements, and the ECA server certificate profile, the following URL is provided: <http://www.disa.mil/infosec/pkieca/serverguidelines.doc>.

4.0. TELECOMMUNICATIONS

4.1. MHS DMZ Gateway

The MHS DMZ is a specialized gateway that will provide limited access to MHS contractors in order to interconnect with DOD government systems such as DEERS, TRICARE ONLINE and the TRICARE Duplicate Claims System in support of the TMA/MHS. This gateway will utilize various electronic devices for security, identification/authorization and controlled access.

4.1.1. All contractor systems that will communicate with DoD systems will interconnect through the established MHS DMZ gateway.

4.1.2. Contractors will connect to this gateway via a contractor procured Internet Service Provider (ISP) connection.

4.2. Contractor Provided IT Infrastructure

4.2.1. Desktop platforms shall support HTTP, HTTPS, Web derived Java Applets, and all software that the contractor proposes to use to interconnect with DoD facilities.

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

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

4.2.4. Every device that is going to connect to the MHS DMZ gateway must have an Internet routable IP address.

4.2.5. It shall be the contractor's responsibility to maintain a backup network connection solution to an ISP in the event their primary link experiences degradation/failure.

4.2.6. Contractor networks shall not exceed 200 ms in one way packet latency and 2% in packet loss for transmissions to any major CONUS Tier 1 ISP peering point.

4.2.7. Troubleshooting and maintenance of Contractor procured ISP connections is the responsibility of the Contractor.

4.3. Form 41 Submission

4.3.1. All Contractors that use the DoD gateways must submit a DISA Form 41 or equivalent for each of their users. The request must clearly delineate the ports and protocols used for each IP address. The form will be completed by the Contractor and submitted to the Government for final processing.

4.3.2. All AISs proposed by the contractor shall comply with "DoD NIPRNET Ports and Protocols Security Technical Guidance (draft)" dated February 2002 ([Chapter 1, Addendum B](#)). Transmission Control Protocol (TCP) services that are "allowed" (coded Green) and "conditional" (coded Yellow) in the "DoD NIPRNET Ports and Protocols Security Technical Guidance (Draft)" document shall be used exclusively in all AISs that the contractor proposes.

4.4. MHS Systems Telecommunications

4.4.1. The primary communication links shall be via **Secure Internet Protocol (IPSEC)** virtual private network (VPN) tunnels between the contractor's primary site and the **MHS DMZ Gateway**. The VPN shall provide an additional level of security by encryption of the data transmission.

4.4.2. To ensure VPN interoperability, the contractor shall use an approved MHS standard VPN device. The current approved VPN device for enterprise corporate connections (e.g., major contractor connections for multiple requirements; Computing Centers) is the Avaya VSU-7500, VPN appliance to establish Internet Key Exchange (IKE) VPN tunnels with the MHS. The standard MHS VPN solution may change over time and the Contractor will be required to upgrade/comply accordingly. The Contractor shall support the integration of this VPN appliance as part of an IKE VPN domain. These VPN appliances shall be configured in accordance with specific VSU configuration guidance provided by the MHS, at the technical specifications meetings following contract award and all VPNs (unless otherwise directed) shall be operated in compliance with Federal Information Processing Standard (FIPS) 140-2 (Chapter 1, Addendum C) (See <http://www.NIST.gov> or http://www.tricare.osd.mil/tmis_new/pcp.htm).

4.4.3. 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 Defense Information Systems Agency (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.

4.4.4. 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 with the primary VPN.

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

4.4.6. Maintenance and repair of Contractor procured VPN equipment shall be the responsibility of the Contractor. Troubleshooting of VPN equipment shall be the responsibility of the Government.

4.5. Contractors located on Military facilities

4.5.1. If the contractor plans to locate personnel on a military facility the contractor must coordinate with the Base/Post/Camp communications office and the MTF.

4.5.2. Contractors located on military facilities 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.

4.5.3. Contractors located on military facilities that require direct connections to their networks shall either:

- Coordinate their network connections to the respective military infrastructure and through the MHS DMZ Gateway with the MTF, Base/Post/Camp, TIMPO, DISA communications personnel.
- If the contractor requires a direct connection back to the contractor's network, they shall provide an isolated IT infrastructure, 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.

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

4.6. DEERS

4.6.1. Primary Site

4.6.1.1. The DEERS primary site is located in Auburn Hills, Michigan and the backup site is located in Seaside, California.

4.6.1.2. The Contractor shall communicate with DEERS through the MHS DMZ Gateway for claims processing.

4.6.1.3. DoD PKI requirements apply for accessing DEERS or the Defense Online Enrollment System (DOES).

4.6.2. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the DOES.

4.7. TMA/TRICARE Encounter Data

4.7.1. Primary Site

The TRICARE Encounter Data (TED) primary site is currently located in Denver, Colorado, and operated by the Defense Enterprise Computing Center (DECC), Denver Detachment for the DISA. Note: The location of the primary site may be changed. The contractor shall be advised should this occur.

4.7.2. 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 TMA, as validated and authorized by TMA. Each contractor on the telecommunication network is responsible for furnishing to TMA 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 point of contact. Contractors shall also furnish a

separate computer center (**Help Desk**) number to TMA which the TMA computer operator can use for resolution of problems related to data transmissions.

4.7.3. TED-Specific Data Communications Technical Requirements

4.7.3.1. Systems Interface Requirements

The Contractor shall communicate with the Government's Data Center through the MHS DMZ Gateway.

4.7.3.2. Communication Protocol Requirements

4.7.3.2.1. 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 is expected to 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

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

4.7.3.2.3. Transmission size is limited to any combination of 250,000 records at one time.

4.7.3.2.4. "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 point of contact 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.

4.7.3.2.5. File Naming Convention

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

4.7.3.2.5.2. First high level qualifier: OCH.

4.7.3.2.5.3. Second high level qualifier: NW. (production only) NWT. (systems integration test)

4.7.3.2.5.4. Third high level qualifier: variable application name assigned by TMA network administration (not to exceed four characters).

4.7.3.2.5.5. Remaining qualifiers: variable per application needs.

4.7.3.2.5.6. The Contractor shall retain source files transmitted over the communications network, to enable immediate isolation and identification for retransmission of the same dataset, for at least seven days. This does not alleviate other data retention requirements imposed by TMA.

4.7.3.2.5.7. Timing

Telecommunication transfers during normal business hours may be adversely affected by normal processing. Therefore, every attempt shall be made to maximize utilization of telecommunications lines by deferring transfers to night-time operation. Ideally, a single file will be transmitted at night. However, there are no restrictions on the number of files that may be transmitted. 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.

4.8. TMA/MHS Referral and Authorization System

4.8.1. Primary Site

The MHS Referral and Authorization System primary site is to be determined.

4.8.2. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the MHS Referral and Authorization System.

4.9. TMA/TRICARE Duplicate Claims System

4.9.1. Primary Site

The TRICARE Duplicate Claims System (DCS) primary site is located in Aurora, Colorado.

4.9.2. Contractor Connection With TMA For The Duplicate Claims System (DCS)

The DCS is planned to operate as a web application. The contractor is responsible for providing 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 TRICARE Operations Manual, Chapters 9 and 10 for DCS Specifications.)

