CHAPTER 1
SECTION 1.1

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 TMA. It covers three major categories of information flowing among the contractor and TMA, 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 functional and technical requirements related to the flow of health care related ADP information between the contractor and TMA. TRICARE Encounter Data (TED) records as well as provider and pricing information must 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 is outlined in Chapter 2, Section 1.2 and the TMA requirements related to submission and updating of pricing information is outlined in Chapter 2, Section 1.3.

1.3. The ADP requirements will incorporate the 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 (COOP)

2.1.1. The contractor shall develop a plan to ensure the COOP of their IT systems and data in support of TRICARE. The COOP plan 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 plan that will enable compliance with all processing standards as defined in the TRICARE Operations Manual, Chapter 1, Section 3.

2.1.2. The contractor will conduct a test of the backup system within the first quarter of the initial health care delivery period and will 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 will be done at least once a year.

2.1.3. The test in the first quarter and the annual test must 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 will be reported to Contract Management Directorate, TMA, 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 Regulation, and all other 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 must 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 must be limited to those persons with a legitimate need to access and use the information. All factors discussed above must 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 an information system. 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)," as stipulated by OMB Circular A-130. The objective of the DITSCAP is to maintain a standardized approach to security C&A for AISs and communication networks. The process is designed to protect and secure those entities that comprise the 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 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 or process MHS SBU information, to undergo an appropriate background investigation and security awareness training before access is granted to a DoD AIS/network or MHS SBU information. Contractors must comply with the current requirements of DoD 5200-R and it's appendices, while performing any TRICARE contract.

Adherence to these requirements provides protection of DoD AISs/networks, information technology (IT) resources and MHS 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, implement processes to provide a C2 level of security for MHS SBU information, and ensure appropriate background investigations are initiated and security awareness training for their personnel is completed before access to DoD AISs/networks or MHS 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

The C&A and Automated Data Processing/Information Technology (ADP/IT) background investigation requirements apply to contractors that manage, design, develop, operate, or access DoD AISs/networks and MHS SBU information. Government Owned Contractor Operated (GOCO) and Contractor Owned Contractor Operated (COCO) AISs/networks that process MHS SBU information are also bound by these requirements. The only exception is when the COCO AIS/network does not have connectivity with a DoD AIS or

network. In this case the DITSCAP requirements do not apply, and other safeguards may be used in lieu of background checks for the investigation process, such as non-disclosure agreements and appropriate training. When completing the DITSCAP investigation, the contractor shall prepare all required documents and modify those documents as necessary to incorporate any Certification Authority (CA) recommendations. Contractor 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 a Trusted Computing Security Evaluation Criteria (TCSEC) C2 level of security for MHS SBU information. Furthermore, the contractor shall prepare, submit, and maintain copies of all required documentation to initiate the investigative process and validate any ADP/IT background investigation requirements. Finally, all C&A and ADP/IT background investigation activities must be coordinated with the MHS IA Program Office, the Contracting Officer's Technical Representative, and the DITSCAP DAA as appropriate.

3.3. Statement Of Work

The contractor shall acquire/develop and maintain DITSCAP documentation to ensure both initial and continued DITSCAP compliance for all contractor AISs/networks processing MHS SBU information. 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 must 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(s)/networks available for testing. Contractor will be required to mitigate all vulnerabilities identified for correction during the risk assessment process. These requirements must be met before fielding the system, and before connectivity to any DoD AIS or network is authorized. The only exception is when the COCO AIS/network does not have connectivity with a DoD AIS or network, when DITSCAP requirements do not apply. However, the contractor shall put in place processes that provide and ensure security protection for any GOCO and/or COCO AISs/networks that process MHS SBU information. When required, 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 MHS SBU information.

3.3.1. DITSCAP Documentation

The contractor shall provide all necessary DITSCAP documentation and take all necessary steps 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 system changes made to the contractor AISs/networks processing MHS SBU information. All AISs and networks that process, sort, transmit, or access sensitive MHS SBU information (including patient medical data) shall require security C&A in accordance with DoD DITSCAP (DoDI 5200.40). The contractor shall produce and finalize all DITSCAP documents

for contractor AISs/networks processing MHS SBU information, including preparation of a System Security Authorization Agreement (SSAA) and required appendices (Deliverable #1). 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 Information Technology Security Evaluation Criteria (ITSEC) 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

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. TCSEC C2 Level Processes

The MHS IA Program Office requires all contractors who manage, design, develop, operate, or access DoD AISs/networks or process MHS SBU information to ensure that an appropriate and consistent level of security is achieved. In order to protect and maintain availability, integrity, authentication, confidentiality, and non-repudiation of MHS SBU information, TCSEC C2 protection is mandatory. The only exception is when the COCO AIS/network does not have connectivity with a DoD AIS or network, when TCSEC C2 requirements do not apply. These requirements are defined in the DoD 5200.28-STD. Therefore, the contractor must:

- Ensure that their personnel receive initial and annual IA training before accessing DoD AISs/networks, and MHS SBU information.
- Protect all contractor AISs/networks and equipment that process MHS SBU information at a level that is equal to, or greater than, the highest level of security protection for any information processed, stored, transmitted, or accessed.
- Implement network security measures to prevent unauthorized access.
- Obtain security (DITSCAP) C&A documents published by DoD for all AISs/networks that process, store, transmit, or access MHS SBU information, if the AIS/Network connects to a DoD system.
- Comply with the requirements for Information Assurance Vulnerability Alert (IAVA) in accordance with the Office of the Deputy Secretary of Defense Policy Memorandum, DoD Information Assurance Vulnerability Alert. 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). MHS Contractor sites should have a structured ability to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten

the security of operations. These incidents must be reported to the CERT immediately.

3.3.4. ADP/IT Requirements

The MHS IA Program Office, in compliance with DoD 5200.2-R - Personnel Security Program, January 1987, requires all contractors who manage, design, develop, operate or access DoD AIS or network to process an appropriate background investigation and security awareness training before access is granted to an AIS or network. The only exception is when a COCO AIS/network does not have connectivity with a DoD IT or network. In this case, background investigations for contractor personnel are not required and other safeguards may be used, such as non-disclosure agreements and appropriate security training. A level of trustworthiness must be established before granting access to MHS SBU information. Therefore, the contractor must:

- Initiate, maintain, and document minimum personnel security investigations appropriate to the individual's responsibilities and access to MHS SBU information.
- 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.
- Immediately deny access to any AIS, network or MHS SBU information to any contractor employee if, at any time, the individual receives an unfavorable NAC adjudication, or if directed to do so by the appropriate government representative for security reasons.
- Ensure all contractor personnel receive IA training before being granted access to DoD AISs/networks, and/or MHS SBU information.

All contractor personnel in positions requiring access to DoD IT systems and networks must be designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III where their duties meet the criteria of these position sensitivity designations as described in the appendix to DoD 5200.2-R. Investigations appropriate for position sensitivity designations are:

ADP/IT I	Background Investigation (BI)
ADP/IT II	DoD National Agency Check Plus Written Inquiries (DNACI) or National Agency Check Plus Written Inquiries (NACI)
ADP/IT III	National Agency Check (NAC) or Entrance National Agency Check (ENTNAC).

Interim Assignment: Individuals, except non-U.S. citizens, to include temporary, intermittent and seasonal personnel, efforts will 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-I:

- Favorable completion of the NAC
- Initiation of an SF85P and Supplemental Questionnaire (when required)

ADP/IT-II:

- A favorable review of local personnel, base/military, medical, and other security records as appropriate
- Initiation of a NACI, as appropriate/favorable review and submission of SF85P and Supplemental Questionnaire (when required)

ADP/IT-III:

- A favorable review of local personnel, base/military, medical, and other security records as appropriate
- Initiation of a NAC, as appropriate/favorable review and submission of SF85P and Supplemental Questionnaire (when required)

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

3.3.4.1. ADP/IT Positions Categories

In establishing the categories of positions, other 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 must be established before granting personnel access to MHS SBU information, DoD AISs/networks or contractor AISs/networks with DoD connectivity, to include:

- ADP/IT-1 Critical Sensitive Position. Those positions in which the individual is responsible for the planning, direction, and implementation of a computer security program; 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.
- ADP/IT-II Noncritical-Sensitive Position. Those positions in which the individual is responsible for the direction, planning, design, operation, or maintenance of a computer system, 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-III Nonsensitive Position. All other positions involved in computer activities.

Each contractor shall be required to complete and submit for appropriate personnel the Standard Form 85-P, "Questionnaire for Public Trust 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.

3.3.4.2. 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 must have a completed investigation and favorable adjudication prior to access. Interim access is not authorized.

3.4. Public Key Infrastructure

The contractor shall comply with DoD policy for enabling networks, web servers and client server applications to make use of the security services made available by the DoD PKI. The Common Access Card (CAC) is the DoD wide primary token platform for PKI certificates. This policy applies to all interfaces with DoD systems. This shall include:

- PK-enabled web applications in unclassified environments
- PK-enabled DoD unclassified networks for hardware token, certificate-based access control

For users of Government Furnished Equipment (GFE) PKI enabled systems (e.g DOES), users will be required to obtain a Common Access Card. To support the issuance of the CAC, the contractor shall have their employees visit a Real Time Automated ID Card System (RAPIDS) facility. Reference the following url for RAPIDS site locations: http://www.dmdc.osd.mil/rsl/. As the volume of CAC issuance increases, the government may expand the number of RAPIDS locations. For information on hardware and software requirements (e.g. card readers and middleware software) required to support the use of the CAC, reference the following url: http://www.dmdc.osd.mil/smartcard/.

4.0. TELECOMMUNICATIONS

4.1. DEERS And MHS Systems Telecommunications

4.1.1. The primary communication links shall be via IPSEC virtual private network (VPN) tunnels between the contractor's primary site and the DEERS primary site and between the contractor's primary site and the MHS primary sites. The VPN shall provide additional level of security by encryption of the data transmission within the network.

4.1.2. To ensure VPN interoperability, the contractor shall use the currently approved MHS standard VPN device. The current approved VPN device is the Avaya VSU-5000, 2000, VSU-1010E, or other fully-compatible Avaya VPN appliance to establish Internet Key Exchange (IKE) VPN tunnels with various MHS sites via commercial or Defense Information Systems Agency (e.g. NIPRNET) connectivity. The standard MHS VPN solution may change over time and the Contractor is expected to upgrade/comply accordingly. The Contractor shall support the integration of this VPN appliance as part of the MHS IKE VPN domain. These VPN appliances shall be configured in accordance with specific VSU configuration

guidance provided by the MHS, and all VPNs (unless otherwise directed) shall be operated in compliance with FIPS 140.

4.1.3. 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.

4.1.4. For backup purposes, an auxiliary VPN device for contractor locations shall be procured and available as a spare.

4.1.5. All long-haul telecommunication lines and communication equipment, up to and including the CSU/DSU, for the interfaces to DEERS and MHS sites shall be ordered, installed, and tested by the contractor. The MHS VPN management authority (e.g. DISA) will remotely configure the VPN once installed and certified as ready for operation by the Contractor.

4.1.6. For connectivity between on-base Contractor locations (e.g. a Contractor LAN on a military installation), the Contractor shall coordinate with the Military installation communications authority (e.g., DISA Base Communications) and the medical facility in the acquisition of secure connectivity from the Contractor's area to the MHS network. TMA, or its designee, is responsible for the implementation of connectivity for on-base or within-the-MTF connectivity to Contractor facilities within the military facility. The Contractor must coordinate their corporate connections directly with the installation but TMA, or its designee, will handle connections to local MTF systems, such as CHCS, if the Contractor facility is within the MTF. If additional communications are required, the Contractor shall coordinate with the medical facility/communications office and procure via the base communications office or DISA.

4.1.7. The Contractor shall be responsible for any security certification documentation as may be required by the Defense Information Systems Agency (e.g. DITSCAP Accreditation) in support of DISA Information Assurance requirements for network connectivity. Further, the Contractor shall provide, on request, detailed network configuration diagrams to support DITSCAP accreditation requirements, and the Contractor shall comply with DISA DITSCAP accreditation requirements regarding the interconnection of Contractor systems and communications infrastructure to DISN networks.

4.1.8. Troubleshooting and maintenance of all Contractor procured longhaul lines communications and communication equipment, up to and including the CSUs/DSUs shall be the responsibility of the contractor.

4.1.9. All network traffic will 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. At the time of the negotiations with base communications personnel or DISA personnel, the contractor will be informed of the specific, applicable security policies with which they must comply.

4.2. DEERS

4.2.1. Primary Site

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

4.2.1.2. The Contractor is responsible for supplying a dedicated primary and backup circuit between their location and DEERS for claims processing. These circuits will meet all telecommunications requirements defined in paragraph 4.1.

4.2.2. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support DOES. All PCs must be configured to support DoD PKI requirements. See paragraph 3.4.

4.3. TMA/TRICARE Encounter Data

4.3.1. Primary Site

The TRICARE Encounter Data (TED) primary site is currently located in Mechanicsburg, Pennsylvania and operated by the Defense Information Systems Agency (DISA). Note: The location of the primary site may be changed. The contractor shall be advised should this occur.

4.3.2. General

The common means of communication between TMA and the contractor for sending and receiving data is a teleprocessing connection. An alternate method may be approved by TMA if there are good reasons to do so. 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 on teleprocessing matters. Contractors shall also furnish a separate computer center number to TMA which the TMA computer operator can use for resolution of problems related to data transmissions.

4.3.3. TED-Specific Data Communications Technical Requirements

4.3.3.1. Front End Processor (FEP) Requirements

4.3.3.1.1. The contractor shall arrange for connections to the government's data processing center. The size and speed of the connection will be based on meeting the government's communications requirements. The specifications of the connection will be coordinated with the government's data processing center. Points of contact at the government's data processing center shall be provided during the technical specifications meetings following contract award.

4.3.3.1.2. Communication systems requirements will be identified by the contractor at the technical specifications meeting following award.

4.3.3.1.3. Integrators shall ensure that interactive traffic has highest priority during normal work hours. (Lights out, automated file transfer technology shall be implemented wherever practical. Human intervention and initiation shall be eliminated to every extent possible. This approach is intended to increase reliability, reduce potential for human error, maximize line utilization, minimize impacts on interactive sessions, and enhance operational efficiency.)

4.3.3.2. Communication Protocol Requirements

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

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

4.3.3.2.2. For interactive session support, TCP/IP communications software incorporating the application TN3270 shall be provided by the contractor.

4.3.3.3. Maintenance And Troubleshooting

4.3.3.3.1. Troubleshooting shall be initiated, either by the government or contractor, for government provided communications equipment. The contractor must provide a POC for this function to the TMA.

4.3.3.3.2. The contractor shall be responsible for troubleshooting and maintaining contractor procured communications equipment.

4.3.3.3.3. At the discretion of the contractor, backup communications equipment may be installed to support contract claim cycle requirements and interactive transaction traffic.

4.3.4. Data Transmission Format Requirements

4.3.4.1. CONNECT:Direct

4.3.4.1.1. A variety of TMA applications shall utilize the CONNECT:Direct communications software.

4.3.4.1.2. CONNECT:Direct does not restrict record lengths or record formats, destination media between host processors, etc. Data conversions occur automatically between platforms founded in ASCII or EBCDIC.

4.3.4.1.3. File organization, record formats, edit specifications, and report formats related to a particular application are identified under appropriate portions of this manual. Reference Chapter 2, Section 2 for record formats, and appropriate, corresponding chapters for edit requirements associated to specific elements within the record formats submitted to TMA.

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

4.3.4.2. User IDs And Passwords

4.3.4.2.1. The goal of TMA security administration is to minimize maintenance of user-IDs and passwords across the network and to accommodate future security strategies through current procedures. All contractors shall comply with DoD & MHS security requirements.

4.3.4.3. Remote User Access To TMA

4.3.4.3.1. TMA shall implement Point Of Entry security in its communications with all remote sites. The network administrator at each remote installation shall contact the TMA network administrator to provide the local user-ID(s), name(s), and telephone number(s) of each individual requiring access to TMA. The TMA network administrator shall use the CONNECT:Direct authorization facility to relate the user id provided by the remote site to an internal user id and password at the TMA data processing installation. System Node ID (SNODEID) overrides shall not be permitted. Three advantages are derived through Point Of Entry implementation:

4.3.4.3.2. The remote user need not be concerned with changing passwords at frequent intervals;

4.3.4.3.3. Potential security breaches through hardcoded passwords are eliminated; and

4.3.4.3.4. Remote user access to CONNECT:Direct can be granted/retracted simply and quickly. The internal user id at TMA shall be highly restricted to standardized high level qualifiers, and shall not have TMA or batch access.

4.3.4.4. TMA Access To Remote Installations

Remote installations shall not require secondary node userid/password from TMA CONNECT:Direct users for the same reasons mentioned above. In those instances where userid/password is in use or planned, a similar security strategy is recommended.

4.3.4.5. "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.

4.3.5. Transmission Development

A pure TCP/IP lights out implementation is the ultimate goal of all automation efforts pertaining to the communications software by eliminating human intervention, and providing reliable and smooth automated interfaces to applications at each site involved. Ideally, the generation, movement, utilization, processing, and reporting of data between remote systems is intended to become virtually transparent. Functional specifications requiring manual input are highly discouraged. In order to facilitate this concept, the contractor shall implement, wherever possible, the TMA file naming convention for data files distributed over the TMA network. To have successful automated processes, all the following must be addressed:

4.3.5.1. File Naming Convention

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

4.3.5.1.2. First high level qualifier: OCH.

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

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

4.3.5.1.5. Remaining qualifiers: variable per application needs.

4.3.5.2. The Contractor:

4.3.5.2.1. 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.

4.3.5.2.2. Is highly encouraged to provide for utilization of the above naming convention standard on their own system for any data files involved in communications with TMA, but is not required to do so when the file being submitted to or retrieved from TMA's input by the contractor to the communication software's automated and standardized processes by variable parameter.

4.3.5.3. Centralization

TMA shall provide the automated process(es) required for implementation of a communications application, with the exception of site specific functions that vary from one

site to another due to implementation of the software's capabilities. An example would be signon/signoff statements for DMBATCH methodologies implemented at that site.

4.3.5.4. Standardization

The contractor shall be afforded the opportunity to provide design and concept input prior to development and implementation of standardized communications processes for each application. Additional instructions pertaining to communications development may be found in the TMA standards.

4.3.5.5. Process Language

Since the effect of communications impacts multiple systems at the contractors and at TMA, all automated processes shall be developed by network administration personnel. Individuals assigned to this function shall be knowledgeable of the capabilities of the software. A network primary and secondary point of contact must be designated at each site (contractors/TMA) to coordinate development, integration, and modification. These individuals shall also be responsible for testing, implementing, monitoring, analyzing error situations, and resolving problems pertaining to communications functions.

4.3.5.6. 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.

4.3.5.7. Frequency

Ideally, data would be accumulated at the source site throughout the workday, with a single file being transmitted at night. However, there are no restrictions on the number of files that may be transmitted in a single day.

4.3.5.8. Initiation

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.

4.3.5.9. Remote Systems Integration Testing Requirements

4.3.5.9.1. In addition to the actual movement of data between two sites, the application interface at each site is a critical piece of automation that severely impacts the success and/or failure of data communications. Interface to distributed applications may be automated, and is highly encouraged wherever practical.

4.3.5.9.2. Integration testing of the applications generating the source file(s) and utilizing the file(s) after transmission is required. These tests shall address at a minimum:

4.3.5.9.3. CPU and communications systems non-availability in excess of 24 hours,

4.3.5.9.4. Scheduled systems maintenance and IPL at each site,

4.3.5.9.5. Isolation of communications functions versus applications processing of data files, especially in respect to delays involving communications,

4.3.5.9.6. Monitoring of active lines/definitions,

4.3.5.9.7. Reasonable lead times for source file preparation,

4.3.5.9.8. Automatic initiation of source and destination file processing, and,

4.3.5.9.9. Adequacy of restart/recovery settings.

4.3.6. Transmission Environment

4.3.6.1. Telecommunications Queue (TCQ)

Management of communications functions shall be accommodated primarily through the software's TCQ. To avoid inadvertent loss of communications processes in progress, warm start is recommended for specification in the CONNECT:Direct initialization parameters.

4.3.6.2. Parallel Session Support

A minimum capability of 2 (two) parallel sessions between a remote site and TMA is requested, but not required. It is assumed that network administration staffs at each site shall configure and tune the environment for maximum performance and balance between all nodes in their network.

4.3.7. Contingency Action Plan

4.3.7.1. Mechanical Or Natural Disasters

If the contractor or TMA is unable to teleprocess data due to mechanical failure or natural disaster and repair time is expected to exceed 24 hours, the contingency action plan shall begin If the failure is on the part of TMA, TMA shall contact the MCSCs via their TMA COR to request data submission via magnetic tape or other digital media, as agreed upon by TMA and the MCSC. If the failure is at the MCSC site, the MCSC shall contact the COR to obtain permission to submit their data to TMA via magnetic tape or other digital media, as agreed upon.

4.3.7.2. Magnetic Tape Processing Or Other Digital Media

Magnetic Tape or other digital media processing requirements shall be agreed upon between the MCSC and the TMA COR at the time of failure.

4.3.7.3. Tape Characteristics

Requirements for tape/digital media characteristics will be determined by TMA at the time the failure is reported.

4.3.7.4. External Label

The MCSC must label the tape/digital media with a minimum of the following information: name of the MCSC, Contractor number, the data set name, and file name. The remaining labeling criteria will be determined by TMA and the MCSC at the time the failure is reported.

4.3.7.5. Shipping Instructions

Shipping address and instructions for the magnetic tape/digital media shall be determined by TMA at the time the failure is reported. All shipments must be packaged in cushioned envelopes or containers.

4.4. TMA/MHS Referral and Authorization System

4.4.1. Primary Site

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

4.4.2. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the MHS Referral and Authorization System. All PCs must be configured to support DoD PKI requirements. (See paragraph 3.4.)

4.5. TMA/TRICARE Duplicate Claims System

4.5.1. Primary Site

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

4.5.2. NIPRNET/INTERNET Connectivity From Contractor To TMA For The Duplicate Claims System

4.5.2.1. The DCS is planned to operate as a web application. The contractor is responsible for providing internal network connectivity to the public internet.

4.5.2.2. All network traffic will be via TCP/IP over NIPRNET connections wherever feasible; otherwise, the public internet will be used. The contractor is responsible for obtaining and maintaining internal and external network connectivity to the NIPRNET/public internet. Please see Addendum A for the NIPRNET Customer Connection Process,

4.5.3. PCs/Hardware

The contractor is responsible for all systems and operating system software needed internally to support the DCS. All PCs must be configured to support DoD PKI requirements. (See the TRICARE Operations Manual, Chapters 9 and 10 for DCS Specifications.)