Chapter 1 Section 1.1

General Automated Data Processing/Information Technology (ADP/IT) Requirements

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 including Defense Enrollment Eligibility Reporting System (DEERS), the contractor systems, and selected Direct Care (DC) information systems.

1.2 Contractors shall comply with TRICARE Management Activity (TMA) guidance regarding access to Department of Defense (DoD), TMA directed ports, protocols and software and web applications. TMA guidance will be issued based on requirements identified by the Office of the Secretary of Defense (OSD), Office of Homeland Security (OHS) or Interagency or Service or Installation and/or Functional Proponency agreements. If multiple requirements exist among the aforementionened entities, contractors shall comply with the most stringent of the requirements.

1.2.1 Contractors shall comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies. Contractors accessing DoD systems shall be provided direction from DoD on connectivity requirements that comply with Ports, Protocols and Services (PPS) in accordance with DoD Instructions. Contractors shall review all DoD, TMA, and Joint Task Force-Global Network Operations (JTF-GNO) Notifications provided by TMA for potential or actual impact on their current system infrastructure and business processes within the designated time frame on the notification. All impacts are to be reported to the Contracting Officer (CO) upon identification, but no later than (NLT) the due date indicated on the notice.

1.2.2 Contractors shall ensure that laptops, flash drives, and other portable electronic devices do not contain Protected Health Information (PHI) unless the device is fully encrypted and accredited per DoD standards.

1.2.3 As portable electronic devices are often used to transmit reference materials and data of a general nature at meetings and conferences, contractors shall ensure that their computer systems can accept and load all such information, regardless of the media used to transmit it. All materials provided to contractors at meetings, workgroups, and/or training sessions sponsored by or reimbursed by the government shall be maintained in accordance with the Records Management requirements in the TRICARE Operations Manual (TOM), Chapter 2.

1.3 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/TMA. TRICARE Encounter Data (TED) records as

well as provider 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 DoD, 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 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.

1.4 For the purposes of this contract, DoD/TMA data includes any information 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/TMA data. DoD/TMA data means any information, regardless of form or the media on which it may be recorded.

1.5 The ADP requirements shall incorporate standards mandated by the DoD Regulation 6025.18-R, dated January 2003, HA Policy 06-010, dated June 27, 2006, Health Insurance Portability and Accountability Act (HIPAA) Security Compliance and the HIPAA Privacy and Security Rule.

1.6 Management and quality controls specific to the accuracy and timeliness of transactions associated with ADP and financial functions are addressed in the TOM, Chapter 1. In addition to those requirements, TMA 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 TMA, contractors are required to participate in the development of a resolution for the issue(s) identified as appropriate. If TMA determines corrective actions are required as a result of government reviews and determinations, the CO will notify the contractor of the actions to be taken by the contractor to resolve the data issues. Corrective actions that must be taken by the contractor to correct data integrity issues, resulting from contractor actions, are the responsibility of the contractor.

2.0 SYSTEM INTEGRATION, IMPLEMENTATION AND TESTING MEETINGS

The TMA 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), Tri-Service Information Management Program Office (TIMPO) and Defense Information System Agency (DISA). The purpose of these meetings is to:

- Review the status of system connectivity and communications.
- Identify new DEERS applications or modifications to existing applications, e.g., DEERS On-line Enrollment System (DOES).
- 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.

TMA provides a standing agenda for the teleconference with the meeting announcement. Additional subjects for the meetings are identified as appropriate. Contractors are required to 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. It is also the responsibility of the contractor to ensure testing activities are completed within the scheduled time frames and any problems experienced during testing are reported via "TestTrack Pro" for review and corrective action by TMA or their designee. Upon the provision of a corrective action strategy or implementation of a modification to a software application by TMA (to correct the problem reported by the contractor), the contractor is responsible for retesting the scenario to determine if the resolution is successful. Retesting shall be accomplished within the agreed upon time frame. Contractors are required to update "TestTrack Pro" upon completion of retesting activities.

TMA will also document system issues and deficiencies into "TestTrack Pro" 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 TMA), the contractor is responsible for retesting the scenario to determine if the resolution is successful. Retesting shall be accomplished within the agreed upon time frame. 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.

Each organization identified shall provide two Point of Contacts (POCs) to TMA to include telephone and e-mail contact and will be used for call back purposes, notification of planned and unplanned outages and software releases. POCs will be notified via e-mail in the event of an unplanned outage using the POC notification list, so it is incumbent upon the organizations to notify TMA of changes to the POC list.

3.0 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.

3.1 Continuity of Operations Plan (COOP)

3.1.1 The contractor shall develop a single plan, deliverable to the TMA 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 and subcontractors in order to continue operations should an actual disaster be declared for their region. The COOP shall ensure the availability of the system and associated data in the event of hardware, software and/or communications failures. The COOP shall also include prime

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. Information specific to connection to the B2B Gateway to and from the relocation/recovery site for operations shall also be included in the COOP. For relocation/recovery sites, contractors must ensure all security requirements are met and appropriate processes are followed for B2B Gateway connectivity. The contractor's COOP will enable 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. The COOP should include 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.

3.2 Annual Disaster Recovery Tests

3.2.1 The prime contractor will coordinate annual disaster recovery testing of the COOP with its subcontractor(s) and the government. Coordination with the government will begin no later than 90 days prior to the requested start date of the disaster recovery test. Each prime contractor will ensure all aspects of the COOP are tested and coordinated with any contractors responsible for the transmission of TRICARE data. Each prime contractor must ensure major TRICARE functions are tested.

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

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

ability to process provider, institutional and non-institutional claims. These test claims will be submitted to the TMA TED benchmark area.

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

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

3.3 DoD Information Assurance Certification And Accreditation Process (DIACAP) Requirements

Contractor Information Systems (IS)/networks involved in the operation of systems of records in support of the MHS requires obtaining, maintaining, and using sensitive and personal information strictly in accordance with controlling laws, regulations, and DoD policy.

3.3.1 Certification and Accreditation (C&A) Process

Contractors shall achieve C&A of all IS that access, process, display, store or transmit DoD Sensitive Information (SI). C&A must be achieved as specified in the contract. Failure to achieve C&A will result in additional visits by assessment teams until C&A is achieved, after which, visits will occur on an annual basis. Return visits by the assessment team may prompt the government to exercise its rights in reducing the contract price. Contract price reductions will reflect costs incurred by the government for each re-assessment of the contractor's information systems, as allowed under contract clause 52.246-4, Inspection of Services-Fixed Price, if deemed appropriate by the CO.

3.3.1.1 The contractor shall safeguard SI through the use of a mixture of administrative, procedural, physical, communications, emanations, computer and personnel security measures that together achieve the requisite level of security established for a Mission Assurance Category III (MAC III) Confidentiality Level (CL) Sensitive system. The contractor shall provide a level of trust which encompasses trustworthiness of systems/networks, people and buildings that ensure the effective safeguarding of SI against unauthorized modifications, disclosure, destruction and denial of service.

3.3.1.2 The contractor shall provide a phased approach to completing the DoD C&A process in accordance with DoD Instruction 8510.01, "DoD Information Assurance Certification and Process (DIACAP)," dated November 28, 2007, within 10 months following the contract award date. C&A requirements apply to all DoD and contractors' ISs that access, process, display, store or transmit DoD information. Contractor shall maintain the MAC III CL Sensitive, Information Assurance (IA) controls defined in reference DoDI 8500.2

The contractor's IS'/networks shall comply with the C&A process established under the DIACAP, or as otherwise specified by the government that meet appropriate DoD IA requirements for safeguarding DoD SI accessed, processed, displayed, maintained, stored or transmitted and used in the operation of systems of records under this contract. The C&A requirements shall be met before the contractor's system is authorized access DoD data or interconnect with any DoD IS or network.

Note: Although the DITSCAP has been superseded by the DIACAP, it should be noted there are no differences in the evaluation criteria. The difference between the processes is specific to reporting requirements by the Information Assurance evaluation team.

Certification is the determination of the appropriate level of protection required for contractor IS'/networks. Certification also includes a comprehensive evaluation of the technical and non-technical security features and countermeasures required for each contractor system/network.

3.3.1.3 Accreditation is the formal approval by the government for the contractor's IS' to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS to operate within the given operational environment with stated interconnections; and with appropriate levels of information assurance security controls. The C&A requirements apply to all DoD IS/networks and contractor's IS/networks that access, manage, store, or manipulate electronic SI data.

3.3.1.4 The contractor shall comply with C&A requirements, as specified by the government that meet appropriate DoD IA requirements. The C&A requirements shall be met before the contractor's system is authorized to access DoD data or interconnect with any DoD IS. The contractor shall initiate the C&A process by providing the CO, not later than 30 days prior to the start of C&A testing, the required documentation necessary to receive an Approval to Operate (ATO). The contractor shall make their IS' available for testing, and initiate the C&A testing four months (120 business days) in advance of accessing DoD data or interconnecting with DoD IS'. The contractor shall ensure the proper contractor support staff is available to participate in all phases of the C&A process. They include, but are not limited to: (a) attending and supporting C&A meetings with the government; (b) supporting/conducting the vulnerability mitigation process; and (c) supporting the C&A team during system security testing and evaluation.

3.3.1.5 Contractors must ensure that their system baseline configuration remains static during initial testing by the C&A team. Contractor's IS' must also remain static for mitigation assessment scans and testing periods. Any reconfiguration or changes to the contractor's information system during the C&A evaluation and testing process may require revision to the system baseline, documentation of system changes and may negatively impact the C&A timeline. Confirmation of the system baseline configuration shall be agreed upon during the definition of the C&A boundary, be signed by the government and the contractor and documented as part of the contractor's System Identification Profile (SIP) and artifacts. Upon completion of all testing and assessments by the C&A team, contractors must notify the IA Directorate, via the CO, of any proposed changes to their IS configuration for review and approval by IA prior to implementation. In order to validate implementation of approved changes does not negatively impact the vulnerability level of a contractor's IS', the C&A team may conduct additional testing and evaluation. During the actual baseline and mitigation assessment scans, the information system must remain frozen. The freeze is only in place during the actual testing periods. Changes between baseline testing and mitigation testing must be coordinated and approved by the MHS IA Program Office prior to implementation.

Any reconfiguration or changes in the system during the C&A testing process may require a rebaselining of the system and documentation of system changes. This could result in a negative impact to the C&A timeline.

3.3.1.6 The C&A process will include the review of compliance with personnel security ADP/IT requirements. The C&A team will review trustworthiness determinations (Background Checks) for personnel accessing DoD sensitive information.

3.3.1.7 Vulnerabilities identified by the government during the C&A process must be mitigated in accordance with the timeline identified by the government. The contractor shall also comply with the MHS DIACAP Checklist. Reference materials may be obtained at http://www.tricare.osd.mil/tmis_new/ia.htm. After contract award date, and an ATO is granted to the contractor, reaccreditation is required every three years or when significant changes occur that impact the security posture of the contractors' information system. An annual review shall be conducted by the TMA IA Office that comprehensively evaluates existing contractor system security posture in accordance with DoD Instruction 8510.01, "DoD Information Assurance Certification and Process (DIACAP)," date November 28, 2007.

3.3.2 Information Assurance Vulnerability Management (IAVM)

The TMA IAVM program provides electronic security notification against known threats and vulnerabilities. The contractor shall comply with the IAVM program requirements to ensure an effective security posture is maintained.

The contractor shall acknowledge receipt of Information Assurance Vulnerability Alerts (IAVA) and Information Assurance Vulnerability Bulletins (IAVB). The contractor shall inform the TMA IAVM Coordinator of applicability or non-applicability of IAVA. The contractor shall implement patch or mitigations strategy and report compliance as specified in IAVA to TMA IAVM Coordinator, if IAVA applies. The contractor shall develop and submit a Plan of Action and Milestones (POA&M) for approval, if IAVA applies, but cannot be mitigated within the compliance time frame. The contractor shall ensure that all required risk mitigation actions are implemented in accordance with associated time line, once POA&M is approved. The contractor shall respond to all TMA IAVM Coordinator queries as to compliance status. The contractor shall ensure TMA IAVM program compliance by their subcontractors.

3.3.3 Disposing of Electronic Media

Contractors shall follow the DoD standards, procedures and use approved products to dispose of unclassified hard drives and other electronic media, as appropriate, in accordance with DoD Memorandum, "Disposition of Unclassified Computer Hard Drives," June 4, 2001. DoD guidance on sanitization of other internal and external media components are found in DoDI 8500.2, "Information Assurance (IA) Implementation, "February 6, 2003 (see PECS-1 in Enclosure 4, Attachment 5) and DoD 5220.22-M, "Industrial Security Program Operating Manual (NISPOM)," Chapter 8).

4.0 HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

On the contract start-work date, the contractor shall be in compliance with the HIPAA Privacy and Security Rules (45 CFR Parts 160 and 164).

Additionally, the contractor shall follow the requirements set forth in the DoD Regulation 6025.18-R, dated January 2003, and the Health Affairs (HA) Policy 06-010, dated June 27, 2006. Contractors shall also establish procedures to ensure the confidentiality, integrity and availability of all beneficiary and provider information in accordance with the requirements of the TOM, Chapter 20, Sections 3 and 4 and the provisions of this Manual and its supporting references.

4.1 Data Use Agreements (DUAs)

The contractor shall enter into a Data Use Agreement (DUA) with TMA in order to be compliant with DoD and HIPAA regulations annually or until their contract is no longer valid. Subcontractors or agents working on behalf of the primary contractor that require the use of, or access to individually identifiable data or protected health information under the provisions of their contract must separately comply, (in coordination with the primary contractor), with referenced DoD and HIPAA regulations and the TMA manuals.

Primary contractors and subcontractors requiring access or use of MHS data must also complete an Account Authorization Request From (AARF) and have an ADP / IT-II. Refer to section 7.3 for Access Requirements.

4.2 Protected Health Information Management Tool (PHIMT)

Contractors shall comply with the HIPAA Privacy Rule requiring covered entities to maintain a history of disclosures of PHI of eligible beneficiaries. Contractors shall also comply with the requirements for the accounting of disclosures and complaint management as specified in DoD 6025.18-R, Sections C7 and C14.4. The PHIMT, a TMA disclosure tracking tool, shall be used by contractors to meet the provisions of the HIPAA Privacy Rule and Privacy Act of 1974. The PHIMT stores information regarding disclosures, complaints, authorizations, restrictions, and confidential communications that are made about or requested by a patient. Contractors and their subcontractors will follow the procedures as outlined in the PHIMT User Guide located on the TMA web site: (http://www.tricare.osd.mil/tmaprivacy/) for disclosure and complaint management and the generation of administrative summary reports. The disclosure management function shall be used to track disclosure requests, disclosure restrictions; accounting for disclosures; authorizations; PHI amendments; Notice of Privacy Practices distribution management; and confidential communications. The complaint management function shall be used to store privacy complaint data. The administrative summary report function shall be used to generate reports and track information found in the disclosure management and complaint management section of the PHIMT. Situation reports may be required to address complaints, inquiries, or unique events related to the disclosure accounting responsibility.

5.0 PRIVACY IMPACT ASSESSMENT (PIA)

Contractors are responsible for the employment of practices that satisfy the requirements and regulations of the E-Government Act of 2002 (Public Law (PL) 107-347, 44 USC CH36 - Section 208); the E-Government Memorandum 03-22 (September 26, 2003) and current DoD PIA Guidance Memorandum at http://www.tricare.mil/TMAPrivacy/Info-Papers-PIAs.cfm.

The PIA is an analysis of how information is handled: (1) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (2) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an

electronic information system, and (3) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy and security risks. The PIA is a due diligence exercise in which organizations identify and address potential privacy risks that may occur during the various stages of a system's lifecycle.

Contractors and their subcontractors shall follow the guidance outlined within the TMA PIA policy and the TMA Privacy Impact Procedures located on the TMA Privacy web site: http://www.tricare.osd.mil/TMAPrivacy/PIA-Submittal-Process.cfm.

Contractors shall initiate a PIA and notify TMA Privacy Office within 10 days of the development, or procurement of information technology systems or projects that collect, maintain, or disseminate information in identifiable form from or about members of the public totaling at least 10 individuals. For existing systems, contractors shall identify systems and develop a plan for completing PIAs, and submit to the TMA Privacy Office within two months following contract award date. Contractors shall use the results of the PIA to identify and mitigate any risks associated with the collection of personal information from the public. Contractors shall submit the PIA using the DoD PIA format and the TMA PIA Completion Procedures to the TMA Privacy Office within 10 days of completion.

The TMA Privacy Office will review and approve the PIA summary submitted by the contractor and make it available to the public upon request via the TMA Privacy web site. The TMA Privacy Office will not publish any PIA summaries that would raise security issues, other concerns or reveal information of a proprietary nature to the contractors. Upon completion of review by the TMA Privacy Office, contractors will be notified of any required corrections. Corrective actions to be provided within time frame designated in notification. The contractors are to review and update PIAs, in coordination with the TMA Privacy Office, if there are system modifications or changes in the way information is handled that increase privacy risk.

6.0 PHYSICAL SECURITY REQUIREMENTS

The contractor shall employ physical security safeguards for IS/networks involved in the operation of its systems of records to prevent the unauthorized access, disclosure, modification, destruction, use, etc., of DoD SI and to otherwise protect the confidentiality and ensure the authorized use of SI. In addition, the contractor shall support a Physical Security Assessment performed by the government of its internal information management infrastructure using the criteria from the Physical Security Assessment Matrix. The contractor shall correct any deficiencies of its physical security posture required by the government. The Physical Security Audit Matrix can be accessed via the Policy and Guidance/Security Matrices section at http://www.tricare.osd.mil/tmis_new/ia.htm.

7.0 PERSONNEL SECURITY ADP/IT REQUIREMENTS

7.1 Policy References

Personnel to be assigned to an ADP/IT position must undergo a successful security screening before being granted access to DoD IT resources. Prior to an employee being granted interim access to DoD sensitive information, the organization must receive notification that the Office of Personnel Management (OPM) has scheduled the employee's investigation. The references and specific guidance below were provided to TMA by the Under Secretary of Defense for Intelligence

(USDI) and the OPM safeguard against inappropriate use and disclosure.

- DoD Directive 8500.1E, "Information Assurance (IA)," October 24, 2002
- DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
- DoD 5200.2-R, "DoD Personnel Security Program," January 1987
- DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
- DoDI 8551.1, "Ports, Protocols, and Services Management (PPSM)," August 13, 2004
- DoD I 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004
- Defense Information Systems Agency (DISA), "Security Technical Implementation Guides"
- DoD 5200.08-R, "Physical Security Program", April 9, 2007
- DoD Assistant Secretary of Defense Health Affairs (ASD (HA)) Memorandum, "Interim Policy Memorandum on Electronic Records and Electronic Signatures for Clinical Documentation," August 4, 2005
- DoD Assistant Secretary of Defense (ASD) Networks and Information Integration (NII) Memorandum "Department of Defense (DoD) Guidance on Protecting Personally Identifiable Information (PII)," August 18, 2006
- "DISA Computing Services Security Handbook", Version 3, Change 1, December 1, 2000
- "Health Insurance Portability and Accountability Act (HIPAA), Security Standards, Final Rule," February 20, 2003
- Military Health System (MHS) Physical Security Assessment Matrix, August 15, 2004
- Military Health System (MHS) DIACAP Checklist, August 2006
- Military Health System (MHS) Security Incident Checklist, September 2005
- Military Health System (MHS) Information Assurance Policy Guidance, March 27, 2007
- MHS IA Implementation Guide No. 2, "Sanitization and Disposal of Electronic Storage Media and IT Equipment Procedures," July 19, 2005
- MSH IA Implementation Guide No. 3, "Incident Reporting and Response Program," March 27, 2007
- MHS IA Implementation Guide No. 5, "Physical Security," July 19, 2005

- MHS IA Implementation Guide No. 6, "Wireless Local Area Networks (WLANs)," July 19, 2005
- MHS IA Implementation Guide No. 7, "Data Integrity" March 27, 2007
- MHS IA Implementation Guide No. 8, "Certification and Accreditation (C&A)," March 27, 2007
- MHS IA Implementation Guide No. 9, "Configuration Management - Security," July 19, 2005
- MHS IA Implementation Guide No. 10, "System Lifecycle Management," July 19, 2005
- MHS IA Implementation Guide No. 11, "DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE)," July 19, 2005
- MHS IA Implementation Guide No. 12, "Information Assurance Vulnerability Management (IAVM) Program," March 27, 2007
- MHS IA Implementation Guide No. 15, "Identity Protection (IdP)," September 14, 2006
- Federal Information Process Standard 140-3, "Draft Security Requirements for Cryptographic Modules," July 13, 2007
- NIST SP 800-34 Contingency Planning Guidance for Information Technology Systems, June 2002
- Privacy Act of 1974
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- DoD 6025.18-R, "DoD Health Information Privacy Regulation," January 2003
- DoD 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM), January 1995 (Change 2, May 1, 2000)
- DoD 5400.11-R " Department of Defense Privacy Program (May 14, 2007)".

The requirements above shall be met by contractors, subcontractors and any others who have access to information systems containing TMA/DoD data protected by the Privacy Act of 1974 and protected health information under HIPAA. Background checks shall be conducted for all ADP/IT contractor personnel who receive, process, store, display, or transmit DoD SI to or from a DoD IS/network prior to being granted access.

7.2 Formal Designations Required

All contractor personnel in positions requiring access to DoD systems or networks, DoD/TMA data, Contractor Owned-Contractor Operated (COCO) systems or networks that contain DoD/TMA data, DEERS, or the B2B Gateway, must be designated as either ADP/IT-I, or ADP/IT-II. ADP / ITs are

Public Trust Positions for which the background investigations result in Trustworthiness Determinations. They are not security clearances. For the purposes of TRICARE contracts, ADP/IT-III trustworthiness certifications are not sufficient for contractor personnel to be granted access to DoD systems or networks, DoD/TMA data, COCO systems or networks that contain DoD/TMA data, DEERS, or the B2B Gateway.

Only TRICARE contractors are permitted to submit ADP/IT background checks in accordance with this policy. Military Service and MTF contractors are not to use this guidance.

7.3 Access Requirements

7.3.1 All contractor personnel accessing the DEERS database or the B2B Gateway must have and use a DoD issued Common Access Card (CAC). In addition, the most current version of the DD 2875 (SAAR) must be completed for each contractor employee requiring access to the B2B Gateway, in accordance with paragraph 11.3. New employees hired by contractors may apply for a CAC upon successful completion of the Federal Bureau of Investigation (FBI) Criminal Background Fingerprint check and receipt of the Investigation Schedule Notice (ISN) from the TMA Privacy Office.

7.3.2 Contractors must notify the TMA Privacy Office via fax or secure e-mail of the submission of the Standard Form (SF) 85Ps (Questionnaire for Public Trust Positions) and the Federal Document (FD) 258 (Fingerprint Form) for new hires and the date submitted to OPM. The notification should include the Name, Social Security Number (SSN), ADP designation, date submitted to OPM, company name, and the contract for which the employee works.

7.3.3 Contractors are required to respond timely to OPM, the Defense Industrial Security Clearance Office (DISCO) or the Defense Office of Hearings and Appeals (DOHA) requests for additional information required during the investigation process. Failure to respond timely to the OPM/DISCO/DOHA will result in the revocation of the CAC by the TMA Sponsor, discontinuation/ termination of the investigation by OPM, and Denial of Access by DOHA. Additionally, contractors must notify the TMA Privacy Office on special issues that require contact with OPM, DISCO, and DOHA.

7.3.4 Contractors are required to ensure personnel viewing data obtained from DEERS or the B2B Gateway, or viewing Privacy Act protected data follow contractor established procedures as required by the TOM, Chapter 1 to assure confidentiality of all beneficiary and provider information.

7.4 ADP/IT Category Guidance

In establishing the categories of positions, a combination of factors may affect the determination. Unique characteristics of the system or the safeguards protecting the system permit position category placement based on the agency's judgment. Guidance on ADP/IT categories is:

7.4.1 **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 the direction and control of risk analysis and/or threat assessment. The required investigation is equivalent to a Single-Scope Background Investigation (SSBI). Responsibilities include:

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

- 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.

- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of $10 million per year or greater; (2) lesser amounts if the activities of the individuals are not subject to technical review by higher authority in the ADP/IT-I category to insure the integrity of the system.

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

- 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.

7.4.2 ADP/IT-II - Non-Critical-Sensitive Position. A position where an individual is responsible for systems' design, operation, testing, maintenance and/or monitoring that is carried out under technical review of higher authority in the ADP/IT-I category, includes but is not limited to: (1) access to and/or processing of proprietary data, information requiring protection under the Privacy Act of 1974, or Government-developed privileged information involving the award of contracts; (2) accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than $10 million per year.

7.4.2.1 Other positions are 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. The required investigation for ADP/IT-II positions is equivalent to a National Agency Check with Law Enforcement and Credit Checks (NACLC).

7.4.2.2 ADP/ITs submitted as a NAC to DSS prior to 2000 were approved as ADP/IT-II/III. Effective 2000, OPM took over the investigation process for TMA. The submission requirements for ADP/IT levels were upgraded as follows: ADP/IT-III is a NAC; ADP/IT-II is a NACLC and; an ADP/IT-I is an SSBI. Investigations submitted before 2000 for a NAC (ADP/IT-II/III) will need to submit a new SF 85P User Form and fingerprint card for a NACLC to be upgraded to an ADP/IT-II.

7.4.3 ADP/IT-III - Non-Sensitive Position. All other positions involved in Federal computer activities. The required investigation is equivalent to a National Agency Check (NAC). This designation is insufficient for granting contractor employee access to DoD IS/Networks, COCO IS/Networks, data and/or DEERS.

Note: The definition of ADP/IT-III is provided for informational purposes only. As previously stated, contractor personnel with ADP/IT-III trustworthiness certifications must be upgraded to an ADP/IT-II NLT October 1, 2004 in order to maintain access to the DEERS database and/or the B2B Gateway.

7.5 Additional ADP/IT Level I Designation Guidance

All TMA contractor companies requiring ADP/IT-I Trustworthiness Determinations for their personnel are required to submit a written request for approval to the TMA Privacy Office prior to submitting applications to OPM. The justification will be submitted to the TMA Privacy Officer, Skyline Five, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041, on the letterhead of the applicant's contracting company. The request letter must be signed by, at a minimum, the company security officer or other appropriate executive, include contact information for the security officer or other appropriate executive, and a thorough job description which justifies the need for the ADP/IT-I Trustworthiness Determination. Contractor employees shall not apply for an ADP/IT-I Trustworthiness Determination unless specifically authorized by the TMA Privacy Officer.

7.5.1 Required Forms

Each contractor employee shall be required to complete and submit the SF 85P, FD 258, and other documentation as may be required by the OPM to open and complete investigations. Additional information may be requested while the investigation is in progress. This information must be provided in the designated time frame or the investigation will be closed/discontinued, and access granted while investigation is underway will be revoked. Instructions and codes for the coversheet will be provided to the contractor by the TMA Privacy Office after contract award. All contractor employees that are prior military should include Copy 4 of the DD214 (Certificate of Release or Discharge from Active Duty) with their original submission. Forms and guidance can be found at http://www.opm.gov/extra/investigate.

Note: The appropriate billing codes will be provided following contract award. Contractors should contact the TMA Privacy Office to obtain the PIPS Form 12 when applying for a Submitting Office Number (SON). The application and billing information must be requested from the TMA Privacy Office. Each primary contracting company is responsible for the submission of the SF 85P for its subcontracting company's employees.

7.5.2 Interim Access (U.S. Citizens Working In The U.S. Only)

All contractor personnel who are U.S. Citizens will receive an OPM ISN from the TMA Privacy Office once the OPM has scheduled the investigation. The TMA Privacy Office sends the ISN to the contracting security officer as validation for interim access after the FBI Criminal Fingerprint check is successfully completed. The contractor security officer may use receipt of the ISN as their authority to grant interim access to DoD/TMA data until a Trustworthiness Determination is made. A contractor employee can apply for a CAC only after the ISN is received.

7.5.3 Temporary Access (U.S. Citizens Only)

Temporary employees include intermittent employees, volunteers, and seasonal workers. Contractors shall obtain an ADP/IT-II Trustworthiness Determination for those positions requiring access to systems containing DoD sensitive information. Interim access is allowed as outlined in paragraph 7.5.2.

7.5.4 Preferred/Partnership Providers Outside of the Continental United States (OCONUS) MHS Facilities (U.S. Citizens Only)

To obtain an ADP Trustworthiness Determination for a preferred/partnership provider the Security Officer of the MTF will contact the TMA Privacy Officer for instructions and guidance on completing and submitting the SF 85P User Form, fingerprint cards and system access. The TMA Privacy Officer will provide guidance on system access upon contact by the Security Officer of the MTF.

7.5.5 ADP/IT Level Trustworthiness Determination Upgrades

7.5.5.1 Contact the TMA Privacy Office if a higher ADP/IT level is required than what was submitted for an employee. In addition, the contractor's security officer must contact the OPM Federal Investigations Processing Center, Status Line, to determine the status of the investigation. OPM can upgrade the level of investigation only if the investigation has not been closed/completed. If the investigation is pending, you may fax a written request to OPM, Attention: Corrections Technician, to upgrade the NACLC to an SSBI. You must provide the name, SSN, and Case Number on your request (Case Number can be found on the ISN). If the SF 85P User Form is missing information, the Correction Technician will call the requester for missing information. Addresses for each organization are shown below.

- TMA Privacy Office, Skyline Five, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041
- OPM Federal Investigations Processing Center, P.O. Box 618, Boyers, Pennsylvania, 16018-0618
- OPM Corrections Department, Federal Investigations Processing Center, P.O. Box 618, Boyers, Pennsylvania, 16018-0618

7.5.5.2 If the investigation has been closed/completed, the original SF 85P Agency User Form (coversheet) must be submitted for the higher ADP/IT level. The SF 85P may be re-used within 120 days of the case closed date, with corrected ADP level code O8B. The letter "I" must be inserted in the Codes box located above C and D on the SF 85P Agency User Form and no fingerprint card is needed. The contractor's Security Officer must update the SF 85P Agency User Form, re-sign and re-date the form in Block P. The individual must line through any obsolete information, replacing it with corrected information and initial all changes made to the SF 85P. The individual must then re-sign and re-date the certification section of the form.

7.5.5.3 If it is beyond the 120 day period, the old SF 85P may be used if all the information is updated and the certification part of the form is re-dated, and re-signed by the individual. A new SF 85P Agency User Form (coversheet) showing the correct ADP/IT level code 30C is required at this time. Each correction/change made to the form must be initialed and dated by the individual.

7.6 Access for Non-U.S. Citizens

7.6.1 Policy

Interim access at Continental United States (CONUS) locations for non-U.S. citizens is not authorized. Non-U.S. citizen contractor employee investigations are not being adjudicated for any Trustworthiness positions, therefore, interim access to DoD ITs/networks is not authorized.

7.6.2 Non-U.S. Citizens/Local Nationals Working At OCONUS MHS Facilities

Non-U.S. Citizens/Local Nationals employed by DoD organizations overseas, whose duties do not require access to classified information, shall be the subject of record checks that include host-government law enforcement and security agency checks at the city, state (province), and national level, whenever permissible by the laws of the host government, initiated by the appropriate Military Department investigative organization prior to employment.

7.7 Transfers Between TRICARE Contractor Organizations

7.7.1 When contractor employees transfer employment from one TRICARE contract to another, while their investigation for ADP/IT Trustworthiness Determination is in process, the investigation being conducted for the previous employer may be applied to the new employing contractor. The new contracting company shall provide the TMA Privacy Office the following information on each new employee from another TRICARE contracting company. This data must be appropriately secured (e.g., secured transmission, registered mail, etc.).

- Name
- SSN
- Name of the former contracting company
- ADP/IT level applied for
- Effective date of the transfer/employment

TMA will verify the status of the Trustworthiness Determination/scheduled investigation for the employee(s) being transferred. If the investigation has not been completed, the TMA Privacy Office will notify OPM to transfer the investigation from the old SON (submitting office number) to the new SON. If the investigation has been completed, OPM cannot affect the transfer. If the Trustworthiness Determination has been approved, the TMA Privacy Office will verify the approval of the Trustworthiness Determination and send a copy to the new contracting company's office.

7.7.2 When a new contractor employee indicates they have a current ADP/IT Trustworthiness Determination (e.g., transfers from another TRICARE contract), the new contracting company shall provide the TMA Privacy Office the following information on the employee. This data must be appropriately secured (e.g., secured transmission, registered mail, etc.).

- Name
- SSN
- Name of the former contracting company
- ADP/IT level
- Effective date of the transfer/employment with the current company

The TMA Privacy Office will verify the status of the individual's ADP/IT Trustworthiness status; if the clearance is current, the TMA Privacy Office will provide the information to the gaining contracting company. If not current, the company will be instructed to begin the ADP investigation process.

7.8 New Contractor Personnel With Recent Secret Clearance

New contractor personnel who have had an active secret clearance within the last two years should not submit a SF 85P to OPM. The contracting company must contact the TMA Privacy Office for verification of previous investigation results.

7.9 Notification Of Submittal And Termination

Contracting companies shall notify the TMA Privacy Office when the Security Officer has submitted the SF 85P to OPM for new employees. Upon termination of a contractor employee from the TRICARE Contract, contracting companies must notify the TMA Privacy Office and OPM. The contracting company shall provide the TMA Privacy Office and OPM the following information on the employee. This data must be appropriately secured (e.g., secured transmission, registered mail, etc.).

- Name
- SSN
- Name of the contracting company
- Termination date

Upon receipt of a denial letter form the TMA Privacy Office, the company security officer shall immediately terminate that contractor's direct access to all MHS information systems, and if the employee was issued a CAC, obtain the CAC from the employee, and confirm to the TMA Privacy Office in writing within one week of the date of the letter that this action has been taken.

8.0 PROCESS FOR SUBMITTING SF 85P, "QUESTIONNAIRE FOR PUBLIC TRUST POSITIONS," FOR CONTRACTOR PERSONNEL WORKING IN PUBLIC TRUST POSITIONS

8.1 In order to obtain access to DoD IT systems or networks, contractor personnel must complete the "Questionnaire for Public Trust Positions," SF 85P. The SF 85P may be obtained at http://www.tricare.mil/tmaprivacy/sf85p.pdf. Completed SF 85Ps must be signed by the TRICARE Contracting Officer's Representative (COR), or a designated government official in the COR's absence and accompanied by a similarly signed cover letter. The OPM will not initiate the investigation if the **first page** of the SF 85P does not include the requisite COR's signature (for an example, see Addendum C, Figure 1.C-1).

8.2 Contractor Responsibilities

8.2.1 Contractor employees are required to accurately complete the SF 85P, with the exception of the portion of the form labeled, "Agency Use Only."

8.2.2 The contractor's Facility Security Officer (FSO) or Public Trust Official (designated contractor official) must complete the top portion of the first page of the SF 85P, blocks "A-O," for

each employee requiring access to a DoD Information Technology system. Instructions for the completion of blocks "A-O" are in Addendum C, Figure 1.C-2, SF 85P Cover Sheet Instructions.

8.2.3 The contractor's FSO must also provide a cover letter (sample provided at Addendum C, Figure 1.C-3) that contains the name(s) of the employee, SSNs, date of birth, and requested ADP level for each contractor employee for which a trustworthiness certification is being requested. The first sheet of each SF 85P and a cover letter should be provided to the COR for signature. Additional attachments shall not be provided.

8.2.4 The COR will sign block "P" of the SF 85P(s) and the corresponding cover letter. Two asterisks (**) should be noted under the COR's signature to denote the presence of "inquiry contact information." The FSO will sign and enter their telephone number at the bottom of the first page of the SF 85P (below block E). The COR will then scan the cover letter and forward the documents via encrypted electronic mail to Ms. Pamela Schmidt, Deputy Director, TMA Privacy Office, at Pamela.Schmidt@tma.osd.mil.

8.2.5 The COR will return the **signed** first page of the SF 85P and the **signed** cover letter to the contractor's FSO.

8.2.6 The FSO will attach the signed first page of the SF 85P to the rest of the questionnaire and the FD258 Fingerprint card and forward the entire package to OPM for processing. The mailing address for OPM is:

Express Package Delivery
U.S. Office of Personnel Management
1137 Branchton Road
Attention: NACLC Team
Boyers, PA 16018

Routine Mail Delivery
U.S. Office of Personnel Management
P.O. Box 618
Attention: NACLC Team
Boyers, PA 16018

8.2.7 OPM will review, accept and schedule the investigation(s) upon receipt of the SF 85Ps unless there is a discrepancy in the information submitted or the form is incomplete. Once the investigations are scheduled, the status will be posted in the Joint Personnel Adjudication System (JPAS) within seven to 10 business days. When the TMA Privacy Office receives the electronic notification of new SF 85P submittals, they will check the JPAS for the investigation schedule for these individuals. The TMA Privacy Office will print a copy of the JPAS printout, indicating the date the investigation is scheduled by OPM and forward it to the contractor's FSO.

8.2.8 In the event of a discrepancy, OPM will mark the form as an "Unacceptable Case Notice" and return it to the TMA Privacy Office. The TMA Privacy Office will return all "Unacceptable Case Notices" to the contractor's FSO for resolution. The FSOs are required to resubmit the corrected copy of the SF 85P to OPM within 10 business days. In the event the contractor employee is no longer with the contractor company or no longer requires a certification of public trustworthiness, the contractor's FSO must notify the TMA Privacy Office immediately.

8.2.9 The TMA Privacy Office will send the COR a spreadsheet with the name(s) of the employee, last four digits of the SSN and the ADP/IT background investigation level for which the contract employee has been scheduled. The receipt of the JPAS printout will serve as notification to the contractor of CAC eligibility.

8.2.10 For information on upgrading requests for trustworthiness determinations in process, see paragraph 7.5.5.1

8.3 Verification Process for Contractor Employees Requiring CACs

Contractors must identify all employees who will require a CAC prior to authorization for access to any DoD Information System. CAC issuance is limited to contractor employees with job requirements for access to DoD Information Systems, or applications not available in the public domain (e.g., via web site to Public users). The following actions shall be taken upon identification of employees who will require a CAC:

8.3.1 For current TRICARE contracts, on official company letterhead, the FSO will submit a list containing the names and SSN for each employee to the COR.

8.3.2 For new contractor employees, on official company letterhead, the FSO will submit a list containing the names and SSN for each employee to the COR.

8.3.3 The COR will scan, encrypt the list (in accordance with TMA specified protocols) and forward to Pamela.Schmidt@tma.osd.mil at the TMA Privacy Office for verification of ADP/IT status.

8.3.4 The TMA Privacy Office will return the verified list to the COR. The COR will notify the contractor they may continue the CAC issuance process for the verified employee(s).

9.0 DOD/MHS INFRASTRUCTURE SECURITY, PORTS, PROTOCOLS AND RISK MITIGATION STRATEGIES

9.1 Contractors will comply with DoD guidance regarding allowable ports, protocols and risk mitigation strategies. The Joint Task Force for Global Network Operations (JTF-GNO) is the responsible proponent for the security of the DoD/MHS Infrastructure. Upon identification of security risks, the JTF-GNO issues JTF-GNO Warning Orders notifying users of scheduled changes for access to the DoD/MHS Infrastructure. TMA will provide contractors with JTF-GNO Warning Orders for review and identification of impacts to their connections with the DoD/MHS. Contractors are required to review Warning Orders upon receipt and provide timely responses to TMA indicating whether the change will or will not affect their connection.

9.2 Upon identification of an impact by the contractor, the contractor shall develop a mitigation strategy to identify the required actions, schedule for implementation and anticipated costs for implementation. The mitigation strategy must be submitted to TMA for review and approval by the JTF-GNO.

9.3 When connectivity requirements that are designated by the Government for the fulfillment of contract requirements are affected by DoD guidance and/or JTF-GNO Warning Orders, mitigation strategies will be developed by the governing agencies.

10.0 PUBLIC KEY INFRASTRUCTURE (PKI)

The DoD has initiated a PKI policy to support enhanced risk mitigation strategies in support of the protection of DoD's system infrastructure and data. DoD's implementation of PKI requirements are specific to the identification and authentication of users and systems within DoD (DoDD 8190.3 and DoDI 8520.2). The following paragraphs provide current DoD PKI requirements.

10.1 User Authentication

All contractor personnel accessing DoD applications, networks and data are required to obtain PKI enabled and Personal Identity Verification (PIV) compliant Government accepted credentials. Such credentials must follow the PIV trust model (FIPS 201) and be acceptable to the government. Currently, to meet this requirement, contractors shall obtain Government-issued CACs. PIV compliant credentials are required for access to DoD systems, networks and data. Alternate sign on access will not be granted. They also allow encryption and digital signatures for information transmitted electronically that includes DoD/TMA data covered by the Privacy Act, HIPAA and SI and network requirements.

10.1.1 Process to Obtain a CAC

10.1.1.1 Contractors shall ensure that all users for whom CACs are requested have initiated the appropriate ADP/IT Personnel Security Requirements (level I or II), including completion of required Government forms (SF 85P and FD 258). The fingerprint check must have been submitted and returned as favorable, and the ISN must be received by the TMA Privacy Office before they can be issued a CAC.

10.1.1.2 In order to obtain a CAC, contractor personnel must first be sponsored by an authorized government representative (sponsor). This representative must be either an active military service member or a federal civilian employee.

10.1.1.3 The contractor shall provide requests for new CACs to the sponsor. These requests shall include necessary personal and employment documentation for all personnel requiring CACs. If 20 or more employees require CACS, the contractor may submit this information electronically to the sponsor. The electronic submission must be protected with a TMA-approved encryption method, and the information provided as a file attachment in XML (eXtensible Markup Language) format for initial startup.

10.1.1.4 The sponsor will provide an access code and password to each individual contractor employee (hereinafter "individual") to the Contractor Verification System (CVS). CVS is a web-based application for the electronic data entry of information into DEERS for approved CAC (contractor and specific non-DoD Federal) applicants. Since the above process will not be used for data submitted electronically, the contractor must insure the data in the XML file is correct prior to submission. The access code and password must be provided the CAC holder in a secure manner, e.g., directly provided to user in a written or verbal format.

10.1.1.5 The individual will then verify personal information in CVS, making corrections as necessary, and entering any missing personal information into CVS (automated DD 1172-2).

10.1.1.6 The sponsor will then review the application and verify the individual employee's ADP/IT status. CAC applications will not be approved if the individual either does not have a current ADP/IT status or has not successfully completed the FBI fingerprint check and/or the TMA Privacy Office has not received the NAC from OPM. If upon review, the sponsor does not approve the application, the sponsor will notify the individual and the appropriate contractor company representative. Once the sponsor approves the individual's application, the sponsor will notify the contractor that he/she can go and obtain his/her CAC.

10.1.1.7 When an individual is notified that their application has been approved, they will go to the nearest Real-Time Automated Personnel Identification System (RAPIDS) location to obtain their CAC. Individuals must bring two forms of identification with them—at least one must be a Government Issued identification card with a photograph (i.e., driver's license/passport). RAPIDS site locations may be obtained at www.dmdc.osd.mil/rsl. The Verifying Official (VO) will verify the identification and capture the biometric data that will be encoded on the CAC.

10.1.2 Initial Contract Start Up

10.1.2.1 When 200 or more contractor employees require CAC issuance, the government may produce the CACs at a Central Issuing Facility (CIF). In order to facilitate the CAC issuance process, the government may also deploy a mobile RAPIDS station to the contractor's site to verify individual employee identity and obtain the biometric data required for the CAC. The site for the mobile RAPIDS station will be determined by the government. Information obtained by the mobile RAPIDS station will be forwarded to the CIF for production of the CAC.

10.1.2.2 The contractor will designate two individuals for the CAC distribution process. The first individual shall be the designated recipient for the CACs that are produced by the CIF; the second will be the recipient for the CAC PINs. Each individual will be responsible for separately distributing the CAC or the PIN, as determined by the responsibility assigned by the contractor.

10.1.3 Reverification

CAC cards for contractors are effective for three years or until the contract end date, whichever is shorter. The sponsor is required to reverify all CAC holders every six months from the date access was granted to each user. To support this requirement, the contractor shall review their personnel lists monthly and submit updated information to the designated Government Official within 10 calendar days of completion. The specific date for the report may be specified by the sponsor.

10.1.4 Lost or Damaged CACs

Lost CACs must be reported to the government representative within 24 hours after the loss is identified. Damaged CACs must be returned to the government. Replacement CACs are obtained from the nearest RAPIDS location.

10.1.5 Termination of Employment

Upon resignation or termination of a user's employment with the contract, the CAC must be surrendered to the designated government representative. CACs must also be surrendered if the individual employee changes positions and no longer has a valid need for access to DoD

systems or networks.

10.1.6 Personal Identification Number (PIN) Resets

Should an individual's CAC become locked after attempting three times to access it, the PIN will have to be reset at a RAPIDS facility or by designated individuals authorized CAC PIN Reset (CPR) applications. These individuals may be contractor personnel, if approved by the government representative. PIN resets cannot be done remotely. The government will provide CPR software licenses and initial training for the CPR process; the contractor is responsible for providing the necessary hardware for the workstation (PC, Card Readers, Fingerprint capture device). It is recommended that the CPR workstation not be used for other applications, as the government has not tested the CPR software for compatibility. The CPR software must run on the desktop and cannot be run from the Local Area Network (LAN). The contractor shall install the CPR hardware and software, and provide the personnel necessary to run the workstation.

10.1.7 E-Mail Address Change

The User Maintenance Portal (UMP) is an available web service that allows current CAC holders to change e-mail signing and e-mail encryption certificates in the event of a change in e-mail addresses. This service is accessible from a local workstation via web services.

10.1.8 System Requirement for CAC Authentication

Contractors shall procure, install, and maintain desktop level CAC readers and middleware. The middleware software must run on the desktop and cannot be run from the LAN. Technical Specifications for CACs and CAC readers may be obtained at www.dmdc.osd.mil/smartcard.

10.1.9 Contractors shall ensure that CACs are only used by the individual to whom the CAC was issued. Individuals must protect their PIN and not allow it to be discovered or allow the use of their CAC by anyone other than him/herself. Contractors are required to ensure access to DoD systems applications and data is only provided to individuals who have been issued a CAC and whose CAC has been validated by the desktop middleware, including use of a card reader. Sharing of CACs, PINs, and other access codes is expressly prohibited.

10.1.10 The contractor shall provide the contractor locations and approximate number of personnel at each site that will require the issuance of a CAC upon contract award.

10.1.11 The contractor shall identify to Purchased Care Systems Integration Branch (PCSIB) and DMDC the personnel that require access to the DMDC Contractor Test environment and/or the Benchmark Test environment in advance of the initiation of testing activities.

10.2 System Authentication

The contractor is required to 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

11.0 TELECOMMUNICATIONS

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

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

11.1.2 In accordance with contract requirements, contractors shall connect to the B2B gateway via a contractor procured Internet Service Provider (ISP) connection. Contractors will assume all responsibilities for establishing and maintaining their connectivity to the B2B Gateway. This will include acquiring and maintaining the circuit to the B2B Gateway and acquiring a Virtual Private Network (VPN) device compatible with the MHS VPN device.

11.1.3 Contractors will complete a current version of the DISA B2B gateway questionnaire providing information specific to their connectivity requirements, proposed path for the connection and last mile diagram. The completed questionnaire shall be submitted to DISA for review and scheduling of an initial technical specifications meeting.

11.2 Contractor Provided IT Infrastructure

11.2.1 Platforms shall support HyperText Transfer (Transport) Protocol (HTTP), HyperText Transfer (Transport) Protocol Secure (HTTPS), Web derived Java Applets, secure File Transfer Protocol (FTP), and all software that the contractor proposes to use to interconnect with DoD facilities.

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

11.2.3 Contractors shall provide full time connections to a TIER 1 or TIER 2 ISP. Dial-up ISP connections are not acceptable.

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

11.3.1 All contractors that use the DoD gateways to access government IT systems must submit the most current version of DD Form 2875 found on the DISA web site: http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage3211.html in accordance with CO guidance. A DD Form 2875 is required for each contractor employee who will access any system on a DoD network. The DD Form 2875 must clearly specify the system name and justification for access to that system.

11.3.2 Contractors shall complete and submit to the TMA Privacy Office the DD Form 2875 for verification of ADP Designation (see paragraph 5.0). The TMA Privacy Office will verify that the contractor employee has the appropriate background investigation completed/or a request for background investigation has been submitted to the OPM. Acknowledgement from OPM that the request for a background investigation has been received and than an investigation has been scheduled will be verified by the TMA Privacy Officer prior to access being approved.

11.3.3 The TMA Privacy Office will forward the DD Form 2875 to the TIMPO for processing; TIMPO will forward DD Form 2875s to DISA. DISA will notify the user of the ID and password via e-mail upon the establishment of a user account. User accounts will be established for individual use and may not be shared by multiple users or for system generated access to any DoD application. Misuse of user accounts by individuals or contractor entities will result in termination of system access for the individual user account.

11.3.4 Contractors 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. Contractors shall provide the TMA Privacy Office with a report of the findings of their review by the 10th day of the month following the review. Reports identifying changes to contractor employee access requirements shall include the name, SSN, Company, IS/network for which access is no longer required and the date access should be terminated.

11.4 MHS Systems Telecommunications

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

11.4.2 The contractor shall place the VPN appliance device outside the contractor's firewalls and shall allow full management access to this device (e.g., in router access control lists) to allow Central VPN Management services provided by the DISA or other source of service as designated by the MHS to remotely manage, configure, and support this VPN device as part of the MHS VPN domain.

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

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

11.4.5 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.

11.5 Contractors Located On MTFs

11.5.1 Contractors located on a military installation who require direct access to government systems shall coordinate/obtain these connections with the local MTF and Base/Post/Camp communication personnel. These connections will be furnished by the government.

11.5.2 Contractors located on military installations that require direct connections to their networks shall provide an isolated IT infrastructure. They shall coordinate with the Base/Post/Camp communications personnel and the MTF in order to get approval for a contractor procured circuit to be installed and to ensure the contractor is within compliance with the respective organizational security policies, guidance and protocols.

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

11.5.3 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 DIACAP accreditation requirements. The contractor shall comply with DIACAP accreditation requirements. All network traffic shall be via TCP/IP using ports and protocols in accordance with current Service security policy. All traffic that traverses MHS, DMDC, and/or military Service Base/Post/Camp security infrastructure is subject to monitoring by security staff using Intrusion Detection Systems.

11.6 TMA/TED

11.6.1 Primary Site

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

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

11.6.2 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 POC. 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.

11.6.3 TED-Specific Data Communications Technical Requirements

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

11.6.3.1 Communication Protocol Requirements

11.6.3.1.1 File transfer software shall be used to support communications with the TED Data Processing Center. CONNECT:Direct is the current communications software standard for TED transmissions. The contractor 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

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

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

11.6.3.1.4 "As Required" Transfers

Ad hoc movement of data files shall be coordinated through and executed by the network administrator or designated representative at the source file site. Generally speaking, the requestor needs only to provide the 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.

11.6.3.1.5 File Naming Convention

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

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

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

11.6.3.1.6 Timing

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

11.6.3.1.6.1 Alternate Transmission

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

11.7 TMA/MHS Referral And Authorization System

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

11.8 TMA/TRICARE Duplicate Claims System

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 TOM, Chapter 9 for DCS Specifications.)

- END -