CHAPTER 1
SECTION 1.1

GENERAL ADP REQUIREMENTS

1.0. GENERAL

1.1. The TRICARE Systems Manual (TSM) defines the contractor's responsibilities related to automated processing of health care information and transmission of relevant data between the contractor and TRICARE Management Activity (TMA). It covers the major categories of information flowing between the contractor, the Department of Defense (DoD), and TMA/Defense Enrollment Eligibility Reporting System (DEERS). These categories include, but are not limited to: health care coverage information and provider 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. Contractors shall comply with TMA guidance regarding access to 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 or Interagency or Service or Installation and/or Functional Proponency agreements. If multiple requirements exist among the aforementioned 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 timeframe on the Notification. All impacts are to be reported to the Contracting Officer (CO) upon identification, but no later than 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 (ADP) information between the contractor and 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 Chapter 2, Section 1.1, the TMA requirements related to submission and updating of provider information are outlined in Chapter 2, Section 1.2 and the TMA requirements related to submission and updating of pricing information are outlined in Chapter 2, Section 1.3.

1.4. 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, Section 4. 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 overage issues). Upon notification of data quality issues by TMA, contractors are required to participate in the development of a resolution to the issue(s) identified, as appropriate.

1.5. 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, 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.

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

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

- 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 5200.2-R, "Personnel Security Program," January 1987
- DoD 5400.11-R, "DoD Privacy Program," May 14, 2007
- DoDI 8500.1, "Information Assurance (IA)," October 24, 2002
- DoD 5015.2-D, "Records Management Program," March 6, 2000
- DoD 5015.02-STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
- DoD 5200.08-R, "Physical Security Program," May 27, 2009

- Homeland Security Presidential Directive 12 (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 25, 2004
- Federal Information Processing Standards Publication 201 (FIPS 201-1), "Personal Identity Verification (PIV) of Federal Employees and Contractors," March 2006.

The requirements above shall be met by contractors, subcontractors and any other individuals who have access to information systems containing TMA/DoD data protected by the Privacy Act of 1974 and Protected Health Information (PHI) under HIPAA.

2.0. SYSTEM INTEGRATION, IMPLEMENTATION, AND TESTING MEETINGS

The TMA Purchased Care Systems Branch hosts regularly scheduled meetings, via teleconference, with contractor and government representatives. Government attendees may include, but are not limited to the 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 of new DEERS applications or modifications to existing applications, e.g., DEERS Online Enrollment System (DOES)
- Issue of software enhancements
- Implement of 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)
- Other activities as appropriate

TMA provides a standing agenda for the teleconference with the meeting announcement. Unique subjects for the meetings are identified as appropriate. Contractors are required to ensure representatives participating in the calls are subject matter experts for meeting 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 timeframe. Contractors are required to update "TestTrack Pro" upon completion of retesting activities.

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, Chapter 1, Section 3 and TOM, Chapter 6, Section 1. Information specific to connection to the Business to Business (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, Section 3 and compliance with enrollment processing and PCM assignment requirements as defined in TOM, Chapter 6, Section 1.

3.2. Annual Disaster Recovery Tests

3.2.1. The prime contractor will coordinate annual disaster recovery testing of the COOP with its subcontractor. All aspects of the COOP are to be tested annually and coordinated with any contractors responsible for the transmission of TRICARE data. Each prime contractor must conduct its annual test once per year, coordinating with their subcontractor(s), ensuring major TRCARE functions are tested annually.

3.2.2. Annual disaster recovery tests will evaluate and validate the prime's COOP sufficiently ensures continuation of operations and the processing of TRICARE data in accordance with the TOM, Chapter 1, Section 3 and TOM, Chapter 6, Section 1. At a minimum, annual disaster recovery testing will include the processing of:

- A sufficient number of TRICARE Prime enrollments in the DEERS contractor test region to demonstrate the ability to comply with the TOM, Chapter 6, Section 1, paragraph 5.4., "The contractor shall electronically submit to DEERS updated records of enrollees and disenrollees using the government furnished system application, DOES."
- Preauthorizations/authorizations in sufficient numbers to demonstrate the ability to function from a recovery/alternate location. This number should be determined based on average daily processing volumes for preauthorizations/authorizations.
- Referrals in sufficient numbers to demonstrate the ability to function from a recovery/alternate location. This number should be determined based on average daily processing volumes for referrals.
- Claims in sufficient numbers to demonstrate the ability to function from a recovery/alternate location. This number may be determined based on average daily processing volumes for claims.

- Claims and catastrophic cap inquiries will be made against production DEERS and the Catastrophic Cap and Deductible Database (CCDD) from the recovery site and the 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 in DEERS, the contractor shall process a sufficient number of claims using the DEERS and CCDD test region.
- TED records will be created for 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 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 conclusion of the test. If the contractor determines that additional testing is required or corrective actions must be taken, the CO shall be provided this information with a report of the results of actions taken 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 DoD Military Health System (MHS) requires obtaining, maintaining, and using sensitive and personal information strictly in accordance with controlling laws, regulations, and DoD policy.

3.3.1. The contractor's IS/networks involved in the operation of DoD systems of records shall be safeguarded through the use of a mixture of administrative, procedural, physical, communications, emanations, computer and personnel security measures that together achieve the same requisite level of security established for DoD IS/networks for the protection of information referred to as "Sensitive Information" (SI) and/or "Controlled Unclassified Information." 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.

3.3.2. Information System (IS)/Networks Certification and Accreditation (C&A)

3.3.2.1. The DIACAP dated July 6, 2006, was established for the authorization of the operation of DoD information systems consistent with the Federal Information Security Management Act (FISMA), Section 3541 of Title 44, United States Code, DoD Directive (DoDD) 8500.1, "Information Assurance (IA)," October 24, 2002, and DoDD 8100.1, "Global

Information Grid (GIG) Overarching Policy," September 19, 2002. This process supersedes DoD Instruction (DoDI) 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP), "December 30, 1997 and DoD 8510.1-M, DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000.

3.3.2.2. The contractor's IS'/networks shall comply with the C&A process established under the DIACAP for safeguarding DoD SI accessed, maintained and used in the operation of systems of records under this contract. 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.

3.3.2.3. Accreditation is the formal approval by the government for the contractors' 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.

3.3.3. C&A Process

The C&A process ensures that the trust requirement is met for systems and networks. Certification is the determination of the appropriate level of protection required for IS/networks. Certification also includes a comprehensive evaluation of the technical and nontechnical security features and countermeasures required for each system/network. Accreditation is the formal approval by the government to operate the contractor's IS/networks in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. In addition, accreditation allows IS/networks to operate within the given operational environment with stated interconnections; and with appropriate level of protection for the specified period. The C&A requirements apply to all DoD IS/networks and contractor's IS/networks that access, manage, store, or manipulate electronic DoD SI data.

3.4. The DIACAP is the standardized approach to the C&A process within DoD. Each IS/network that undergoes DIACAP must have required security controls in place, must have documented the security components and operation of the IS/network and must successfully complete testing of the required security controls. The contractor shall ensure DIACAP documentation is available for review and is accurate. The contractor shall also implement an information assurance vulnerability management program providing mitigation from known vulnerabilities. The contractor, as part of that program, shall provide a primary and secondary point of contact for the MHS Information Assurance Vulnerability Alert (IAVA) Monitor. The point of contact shall provide, upon receipt of a vulnerability message, an acknowledgment of receipt. The contractor shall mitigate the vulnerability, and upon mitigation, report compliance. Receipt and compliance messages to the government shall occur within the stipulated window, as stated in the vulnerability message, and be directed to the MHS IAVA Monitor. Mitigation compliance for IA vulnerabilities shall be assessed on an annual basis.

3.4.1. The contractor shall execute the DIACAP process by providing, for receipt by the CO within 60 days following contract award, the required documentation necessary to

receive an Approval to Operate (ATO), and making their IS/networks available for testing and initiate testing 120 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. Contractors must confirm that their system baseline configuration remains static during the initial testing.

3.4.2. Confirmation of system baseline configuration shall be agreed upon during the definition of the C&A boundary and be signed by the government and the contractor and documented as part of the System Identification Profile (SIP) and artifacts.

3.4.3. 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.

3.4.4. The contractor shall be required to mitigate the vulnerabilities identified for correction during the C&A process. The above requirements shall be met before interconnecting with any DoD IS/network or electronic access to DoD SI is authorized. The contractor shall comply with the MHS DIACAP Checklist. Reference material and DIACAP tools can be obtained at http://www.tricare.mil/tmis_new/ia.htm.

3.4.5. After contract award date, and an Approval to Operate (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 Information Assurance Office that comprehensively evaluates existing contractor system security posture in accordance with FISMA.

3.5. 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)

The contractor shall be compliant with the HIPAA privacy and security rules (45 Code of Federal Regulations (CFR), Parts 160 and 164), and corresponding DoD regulations.

5.0. 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 identified by the government of its physical security posture. The Physical Security Audit Matrix can be accessed via the Policy and Guidance/ Security Matrices section at http://www.tricare.mil/tmis_new/ia.htm.

6.0. PERSONNEL SECURITY ADP/IT REQUIREMENTS

Personnel to be assigned to positions that require ADP/IT-I or ADP/IT-II designation shall undergo a successful security screening before being granted access to DoD Information Technology (IT) systems that contain sensitive data.

6.1. Formal Designations Required

In accordance with DoD regulations, contractor personnel in positions requiring access to the following must be designated as ADP/IT-I or ADP/IT-II:

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

6.1.1. Employee Prescreening

6.1.1.1. Contractors shall conduct thorough reviews of information submitted on an individual's application for employment in a position that requires either an ADP/IT background check or involves access via a contractor system to data protected by either the Privacy Act of 1974, as amended or the HHS HIPAA Privacy and Security Final Rule. This prescreening shall include reviews that:

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

6.1.1.2. The prescreening shall be conducted as part of the preemployment screening and can be performed by the contractor's personnel security specialists, human resource manager, hiring manager, or similar individual.

6.2. Special Access Requirements

6.2.1. New employees hired by contractors are granted interim access upon validation that an investigation has been scheduled by OPM and completion of an Advanced Fingerprint Report by the Federal Bureau of Investigation (FBI) with favorable results.

6.2.2. Contractors shall notify the TMA Personnel Security Division (PSD) of the submission of SF 85P, "Questionnaire for Public Trust Positions," for new hires and the date submitted. In addition, contractors shall respond timely to the OPM for requests for additional information required for the processing of the SF 85P. Failure to respond timely to the OPM will result in the revocation of interim access.

6.3. ADP/IT Category Guidance

The following guidance should be used when determining an individual's specific ADP/IT level:

6.3.1. **ADP/IT-I**. Those positions in which an 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. The required investigation is equivalent to a Single-Scope Background Investigation (SSBI).

For ADP/IT-I Positions of Public Trust, OPM requires that individuals submit a new SF 85P and FBI FD258 Fingerprint Card every 5 years. The Facility Security Officer shall track this information and initiate new investigations, as required by DoD regulations.

6.3.2. **ADP/IT-II**. Those positions in which an 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 than the ADP/IT-I category to ensure the integrity of the system. The required investigation is equivalent to the National Agency Check with Local Agency Check and Credit Check (NACLC).

For ADP/IT-II Positions of Public Trust, OPM requires that individuals submit a new SF 85P and FBI FD258 Fingerprint Card every 10 years. The Facility Security Officer shall track this information and initiate new investigations, as required by DoD regulations.

6.4. Additional ADP/IT Level Designation Guidance

All TMA contractors requiring ADP/IT-I Trustworthiness Determinations for their personnel shall submit a written request for approval to the TMA PSD prior to submitting applications to OPM. The justification shall be submitted to the TMA Office of Administration, Personnel Security Division, 5111 Leesburg Pike, Suite 810, Falls Church, Virginia, 22041-3206, on the letterhead of the applicant's contracting company. The request letter shall 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 that justifies the need for the ADP/IT-I Trustworthiness

Determination. Contractors shall not apply for an ADP/IT-I Trustworthiness Determination unless specifically authorized by the TMA PSD.

6.5. Requests For Additional Information

Additional information specific to the application may be requested while the investigation is in progress. This information shall be provided in the designated timeframe or the investigation may be closed.

The appropriate billing code will be provided following contract award. Contractors shall contact the TMA PSD to obtain the PIPS Form 12 when applying for a Submitting Office Number (SON). The application and billing information shall be requested from the TMA PSD. Each contracting company or subcontracting company shall contact the TMA PSD individually for this information.

6.6. Transfers Between Contractor Organizations

6.6.1. When contractor employees transfer employment from one TMA contract to another TMA contract 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 notify the TMA PSD to provide notification of the new employee from a previous TRICARE contractor. The notification must contain the following:

- Name
- Name of the former employing contractor
- ADP/IT level applied for
- Effective date of the transfer/employment

Notifications shall be submitted via secure fax at (703) 681-3934 or United States (US) Postal Service.

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

6.7. New Contractor Personnel With Recent Secret Clearance Or Prior US Military Service

New contractor personnel who have had an active secret clearance within the last two years do not need to submit a SF 85P. The contracting company shall send the individual's name, SSN, and the date of last employment where the security clearance was used to the TMA PSD. The contractor shall send this information via secure fax at (703) 681-3934 or US Postal Service to:

TRICARE Management Activity
Office of Administration
Personnel Security Division
5111 Leesburg Pike Suite 810
Falls Church, VA 22041-3206

6.8. Notification Of Submittal And Termination

Contracting companies shall notify the TMA PSD 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 shall notify the TMA PSD. The contracting company shall provide the TMA PSD the following information on the employee. This data shall be appropriately secured (e.g., secure fax at (703) 681-3934 or US Postal Service, etc.):

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

Upon receipt of a denial letter from the TMA PSD, the facility security officer shall immediately terminate the individual's direct access to all MHS information systems, secure and confiscate any CAC issued to the terminated individual, and return to TMA PSD.

6.9. Process For Submitting SF 85P, "Questionnaire For Public Trust Positions," For Contractor Personnel Working In Public Trust Positions

6.9.1. In order to obtain access to DoD IT systems or networks, contractor personnel must complete the SF 85P. The SF 85P may be obtained at http://www.opm.gov. Completed SF 85Ps will 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. OPM will not initiate the investigation if the Block P of the Agency User Block in the SF 85P is not signed by the requisite COR (for an example, see Addendum C, Figure 1-C-1).

6.9.2. Contractor Responsibilities

6.9.2.1. The contractor's Facility Security Officer (FSO) or Public Trust Official (designated contractor official) shall 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.

6.9.2.2. The contractor's FSO shall also provide a cover letter (sample provided at Addendum C, Figure 1-C-3) that contains the name(s) of the employee(s), SSN(s), date(s) of birth, and requested ADP level for each contractor employee for which a trustworthiness determination is being requested. The first sheet of each SF 85P and a cover letter shall be provided to the COR for signature.

6.9.2.3. The FSO shall 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

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

6.9.2.5. If the contractor FSO does not receive a copy of the individual's JPAS summary within 10 business days from the date of submission to OPM, the contractor FSO shall contact the TMA PSD for further information. The contractor FSO shall notify the TMA PSD via secure fax at (703) 681-3934 or US Postal Service. Inquiries shall include the employees name, SSN and nature of the inquiry.

6.9.2.6. In the event of a discrepancy, OPM will mark the form as an "Unacceptable Case Notice" and return it to the TMA PSD. The TMA PSD will return all "Unacceptable Case Notices" to the contractor's FSO for resolution. The FSOs shall 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 determination of public trustworthiness, the contractor's FSO shall notify the TMA PSD immediately.

6.9.3. For information on upgrading requests for trustworthiness determinations in process, see paragraph 6.4.

6.10. Electronic Questionnaires For Investigations Processing (e-QIP)

All applications for Public Trust Positions shall be submitted using current trustworthiness process pending phase-in of the e-QIP system. E-QIP is a secure OPM web-based automated system that facilitates the processing of the following Standard Forms (SFs): SF 85 "Questionnaire for Non-Sensitive Positions," SF 85P, "Questionnaire for Public Trust Positions," and SF 86, "Questionnaire for National Security Positions."

During the e-QIP phase-in period, each FSO shall complete the e-QIP training. The Agency Administrator for TMA Office of Administration (OA) PSD will grant access to the e-QIP portal. Before accounts may be created, the FSO shall provide the following information to the TMA PSD:

- SSN
- Full Name
- Date of Birth
- Place of Birth

7.0. PUBLIC KEY INFRASTRUCTURE (PKI)

7.1. 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. The PKI program will be phased into contracts over a period of time to be determined by the Government. The CO will provide contractors with written notification of PKI requirements that must be met in order to continue access to TMA direct systems and/or web applications as they are PKI-enabled and activated.

7.2. For individual authentication required to access to DoD PKI-enabled applications and to allow for encrypted e-mail communications between contractors and the DoD, contractors may be provided a limited number of CACs that contain PKI certificates to be used during the phase-in of PKI requirements. CACs will be limited to individual use and shall not be shared among multiple users, and will be used only for Government designated purposes. Misuse of a CAC will result in revocation of access for the user (and the CAC) and will not be reissued for the contract. Credentials revoked for misuse will be lost for the life of the contract and may not be reissued to another employee.

7.2.1. CACs are valid for three years from the issuance date, until the end date of the contract, or upon termination of employment under the contract for which the CAC was issued, whichever is the earliest date. The CO will provide contractors with written notification of the process to be followed to obtain and use CACs.

7.2.2. CACs remain the property of the Government. Should the designated individual's employment on the contract end prior to the expiration of their CAC, it is the responsibility of the contractor to return the CAC to the Government. Contractors must notify the CO of the need to obtain a CAC for the employee's replacement. A CAC may be issued to the replacement employee provided the individual meets the requirements for assignment and the CAC was not revoked due to misuse by the previous employee.

7.2.3. DoD applications which may be PKI-enabled and reside either on a DoD Local Area Network or a DoD private (restricted access, e.g., username/password) Web server include, but are not limited to, the following:

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

- Civilian PCM Panel Reassignment [DEERS Client/Server application]
- Catastrophic Cap and Deductible/Fee Research [DEERS Web application]
- PCM Research [DEERS Web application]
- DEERS Security Web Application [Web application]
- OHI/SIT [DEERS Web application]
- Direct Care PCM Panel Reassignment [Web application]
- Contractors Resource Center [Web application]

7.2.4. For continued access to DoD PKI-enabled applications during the phase-in process, individual applications may include bypass mechanisms to be used by contractors. These applications will be identified via written notification by the CO and will include information specific to the access procedure to be followed. The CO will also notify the contractor in writing of the termination date of the interim access process at which point only access using PKI will be allowed.

7.3. Contractor personnel who are issued CACs per written direction of the CO will be eligible to receive their certificates from the government.

7.4. PKI certificates may be required for contractor personnel that access Government systems, and/or used for encryption of e-mail and digital signatures. If a system allows the use of External Certification Authorities (ECA) PKI certificates for contractors accessing Government systems from non-.mil domains the certificates may be purchased through DoD approved ECAs.

7.4.1. See http://iase.disa.mil/pki/eca for a list of DoD approved ECAs.

7.4.2. ECA PKI certificates are not a substitute for CAC PKI certificates when CAC PKI certificates are required to access a DoD IT system.

7.5. Additionally the contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers involved in the following system-to-system or host-to-host interfaces. These interfaces include, but are not limited to, the following:

- Contractor systems for claims eligibility inquiries and responses and DEERS
- Contractor systems and the TED Processing Center

7.6. The contractor is responsible for renewing the PKI credential, either the ECA or CAC, in accordance with written procedures provided by the CO in order to maintain access to required applications and/or for the encryption of e-mail and digital signatures.

8.0. TELECOMMUNICATIONS

8.1. MHS Demilitarized Zone (DMZ) Managed Partner Care B2B Gateway

8.1.1. All contractor systems that will communicate with DoD systems will interconnect through the established MHS B2B gateway. For all Web applications, contractors will connect to a DISA-established Web DMZ.

8.1.2. In accordance with contract requirements, MCS contractors will 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.

8.1.3. It is anticipated that modifications will also allow provisioning of dedicated point-to-point commercial circuits to the B2B gateway. The DISA B2B Gateway is a redundant service that is provisioned at two locations. If contractors require high availability, they may acquire redundant circuits to both locations.

8.2. Contractor Provided IT Infrastructure

8.2.1. Platforms shall support HTTP, HTTPS, Web derived Java Applets, client/server, FTP, secure FTP, and all software that the contractor proposes to use to interconnect with DoD facilities.

NOTE: The DoD is phasing out the use of FTP. Upon notification from the government, the contractor shall cease using FTP and begin utilizing the FTP alternative stipulated by the government.

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

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

8.3. DISA Form 41 Submission

All contractors that use the DoD gateways to access government systems must submit a DISA Form 41 or equivalent in accordance with CO guidance. In addition, Form 41s are required for each system administrator responsible for each host-to-host interface. Contractors shall complete and submit to TMA one Form 41 for their organization, attached to which shall be a listing of those individuals for whom background checks have been completed or for whom requests/applications for background checks have been completed, submitted to the OPM, and acknowledgements have been received from OPM that the applications are complete and are pending action by OPM. The request must clearly delineate the ports and protocols used for each IP address. The contractor shall complete the form and submit it to the government for final processing.

8.4. MHS Systems Telecommunications

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

8.4.2. 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.

8.4.3. 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.

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

8.4.5. 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.

8.5. Contractors Located On MTFs

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

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

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

- Coordinate their network connections to the respective military infrastructure and through the MHS B2B Gateway.
- If the contractor requires a direct connection back to the contractor's network, they shall provide an isolated IT infrastructure, coordinate with the Base/Post/Camp communications personnel and the MTF in order to get approval for a contractor procured circuit to be installed and to ensure the contractor is within compliance with the respective organizational security policies, guidance and protocols. Note: In some cases, the contractor may not be allowed to establish these connections due to local administrative/security requirements.

8.5.4. The contractor shall be responsible for all security certification documentation as required to support DoD Information Assurance requirements for network interconnections. Further, the contractor shall provide, on request, detailed network configuration diagrams to

support 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.

8.6. DEERS

8.6.1. Primary Site

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

8.6.1.2. The contractor shall communicate with DEERS through the MHS B2B Gateway.

8.6.2. PCs/Hardware

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

8.7. TMA/TED

8.7.1. Primary Site

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

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

8.7.2. General

The common means of administrative communication between Government representatives and the contractor is via telephone and e-mail. An alternate method may be approved by TMA, as validated and authorized by TMA. Each contractor on the telecommunication network is responsible for furnishing to TMA at the start-up planning meeting (and update when a change occurs), the name, address, and telephone number of the person who will serve as the technical Point Of Contact (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.

8.7.3. TED-Specific Data Communications Technical Requirements

8.7.3.1. Systems Interface Requirements

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

8.7.3.2. Communication Protocol Requirements

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

Sterling Commerce
4600 Lakehurst Court
P.O. Box 8000
Dublin, OH 43016-2000 USA
http://www.sterlingcommerce.com/solutions/products/ebi/connect/direct.html
Phone: 614-793-7000 / Fax: 614-793-4040

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

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

8.7.3.2.4. "As Required" Transfers

Ad hoc movement of data files shall be coordinated through and executed by the network administrator or designated representative at the source file site. Generally speaking, the requestor needs only to provide the point of contact at the remote site, and the source file name. Destination file names shall be obtained from the network administrator at the site receiving the data. Compliance with naming conventions used for recurring automated transfers is not required. Other site specific requirements, such as security constraints and pool names are generally known to the network administrators.

8.7.3.2.5. File Naming Convention

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

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.

8.7.3.2.5.2. 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.

8.7.3.2.5.3. Timing

Telecommunication transfers during normal business hours may be adversely affected by normal processing. Therefore, every attempt shall be made to maximize utilization of telecommunications lines by deferring transfers to night-time operation. Ideally, a single file will be transmitted at night. However, there are no restrictions on the number of files that may be transmitted. Under most circumstances, the source file site shall initiate automated processes to cause transmission to occur. With considerations for timing and frequency, activation of transfers for each application shall be addressed on a case by case basis.

8.7.3.2.5.4. Alternate Transmission

Should the contractor not be able to transmit their files through the normal operating means, the contractor should notify TMA (EL/DS Operations) that they will be sending their files by tape via overnight delivery.

8.8. TMA/MHS Referral And Authorization System

8.8.1. Primary Site

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

8.8.2. PCs/Hardware

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

8.9. TMA/TRICARE DCS

8.9.1. Primary Site

The TRICARE DCS primary site is located in Aurora, Colorado.

8.9.2. Contractor Connection With TMA For The DCS

The DCS is planned to operate as a web application. The contractor is responsible for providing internal connectivity to the public Internet. The contractor is responsible for all systems and operating system software needed internally to support the DCS. (See the TOM, Chapters 9 and 10 for DCS Specifications.)