



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS

16401 EAST CENTRETECH PARKWAY
AURORA, COLORADO 80011-9066

TRICARE
MANAGEMENT ACTIVITY

PCSIB

CHANGE 69
7950.1-M
NOVEMBER 5, 2008

PUBLICATIONS SYSTEM CHANGE TRANSMITTAL
FOR
TRICARE SYSTEMS MANUAL (TSM)

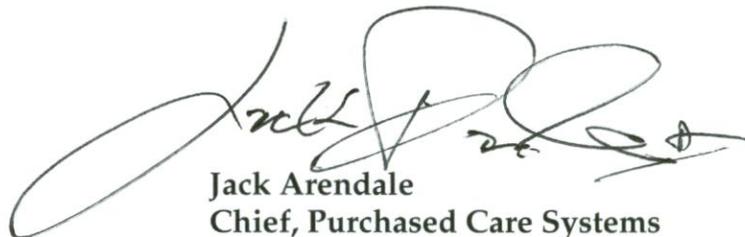
The TRICARE Management Activity has authorized the following addition(s)/
revision(s) to 7950.1-M, reissued August 2002.

CHANGE TITLE: PROCESS FOR SUBMITTING STANDARD FORM (SF) 85P

PAGE CHANGE(S): See page 2.

SUMMARY OF CHANGE(S): This change identifies the process to be followed for
the SF 85P "Questionnaire for Public Trust Positions."

EFFECTIVE AND IMPLEMENTATION DATE: Upon direction of the Contracting
Officer.



Jack Arendale
Chief, Purchased Care Systems
Integration Branch

ATTACHMENT(S): 22 PAGES
DISTRIBUTION: 7950.1-M

CHANGE 69
7950.1-M
NOVEMBER 5, 2008

REMOVE PAGE(S)

INSERT PAGE(S)

CHAPTER 1

Table of Contents, page i
Section 1.1, pages 7 - 10 and 13 - 20
★ ★ ★ ★ ★ ★

Table of Contents, page i
Section 1.1, pages 7 - 10 and 13 - 22
Addendum C, pages 1 - 4

CHAPTER 2

Section 2.2, pages 9 and 10

Section 2.2, pages 9 and 10

CHAPTER 3

Section 1.4, page 7

Section 1.4, page 7

GENERAL ADP REQUIREMENTS

SECTION	SUBJECT
1.1	GENERAL ADP REQUIREMENTS
	1.0. General
	2.0. System Integration, Implementation, And Testing Meetings
	3.0. ADP Requirements
	4.0. Health Insurance Portability and Accountability Act (HIPAA)
	5.0. Physical Security Requirements
	6.0. Personnel Security ADP/IT Requirements
	7.0. Process For Submitting SF 85P, "Questionnaire For Public Trust Positions," For Contractor Personnel Working In Public Trust Positions
	8.0. Public Key Infrastructure (PKI)
	9.0. Telecommunications
ADDENDUM A	DoD 5200.2-R, JANUARY 1987 - AP6. APPENDIX 6
ADDENDUM B	FIPS PUB 140-2 - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES
ADDENDUM C	FIGURES
	FIGURE 1-C-1 Standard Form (SF) 85P Sample
	FIGURE 1-C-2 SF 85P Cover Sheet Instructions
	FIGURE 1-C-3 Cover Letter For Facility Security Officer/Public Trust Official

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 as implemented by the Department of Health and Human Services (DHHS) final rule on Health Insurance Reform: Security Standards (45 Code of Federal Regulations, Parts 160, 162, and 164), effective April 21, 2003. Although the compliance date established by the DHHS Final Rule is April 21, 2005, the contractor shall be in compliance with the requirements of the final rule at the start-work date of this contract.

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

6.1. Policy References

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

Secretary of Defense for Intelligence (USDI) and OPM safeguard against inappropriate use and disclosure.

- 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 5220.22-M, "National Industrial Security Program Operating Manual" (NISPOM), January 1995 (Change 2, May 1, 2000)
- DoDI 8500.1, "Information Assurance (IA) (October 24, 2002)."

The requirement above must be met by contractors, subcontractors and others who have access to information systems containing information protected by the Privacy Act of 1974 and protected health information under HIPAA. Background checks are required for all ADP/IT personnel who receive, process, store, display, or transmit SI.

6.2. Formal Designations Required

All contractor personnel in positions requiring access to DoD IS/networks or Contractor Owned-Contractor Operated (COCO) IS/networks interconnected with DoD IS/networks must be designated as ADP/IT-I, ADP/IT-II, or ADP/IT-III. Only TRICARE contractors are permitted to submit ADP/IT background checks in accordance with this policy. Military Service and Military Treatment Facility (MTF) contractors are not to use this guidance.

6.3. Special Access Requirements

6.3.1. All contractor personnel accessing the DEERS database or the B2B Gateway must have an ADP/IT-II Trustworthiness Determination. Contractor personnel currently working in DEERS with an ADP/IT-III or an interim ADP/IT-III Trustworthiness Determination must upgrade to an ADP/IT-II or interim ADP/IT-II Trustworthiness Determination no later than October 1, 2004. Access to the DEERS database or the B2B Gateway for contractor personnel with ADP/IT-III Trustworthiness Determinations will no longer be granted after October 1, 2004.

6.3.2. New employees hired by contractors are granted interim access for six months upon submission of the **Standard Form (SF) 85P** and fingerprint cards to the OPM. Contractors must notify the TMA Privacy Office of the submission of SF 85Ps for new hires and the date submitted. In addition, Contractors are required to 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 by the TMA Privacy Office.

6.3.3. 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, Section 4, paragraph 3.0.](#), to assure confidentiality of all beneficiary and provider information. The contractor is required to

assure the rights of the individual are protected in accordance with the provisions of the Privacy Act, HIPAA, and HHS Privacy regulation and to prevent the unauthorized use of TMA files.

6.4. 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 judgement. Guidance on ADP/IT categories is:

6.4.1. 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 DAA that involve a relatively high risk for causing severe damage to persons, property or systems, or potential for realizing a significant personal gain.

6.4.2. 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.

6.4.2.1. 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 is equivalent to a National Agency Check with Law Enforcement and Credit (NACLC).

6.4.2.2. 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 NACLIC and; an ADP/IT-I is a 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 NACLIC to be upgraded to an ADP/IT-II.

6.4.3. **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).

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 no later than October 1, 2004 in order to maintain access to the DEERS database and/or the B2B Gateway.

6.5. Additional ADP/IT Level Designation Guidance

All TMA contractors 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, 20041, 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. Contractors shall not apply for an ADP/IT-I Trustworthiness Determination unless specifically authorized by the TMA Privacy Officer.

6.5.1. Required Forms

Each contractor shall be required to complete and submit the necessary standard forms, fingerprint forms, 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 timeframe or the investigation may be closed. 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 code 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 contracting company or subcontracting company must contact the TMA Privacy Office individually for this information.

6.7. Transfers Between Contractor Organizations

6.7.1. When contractor employees transfer employment from one government contractor 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 will send an Excel spreadsheet to the TMA Privacy Office to provide notification of the addition of the new employee from a previous TRICARE contractor. The spreadsheet must contain the following:

- Name
- Social Security Number (SSN)
- Name of the former employing contractor
- ADP/IT level applied for
- Effective date of the transfer/employment

6.7.2. 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, TMA will verify the approval of the Trustworthiness Determination and send a copy to the new employing contractor's office.

6.8. New Contractor Personnel With Recent Secret Clearance

New contractor personnel who have had an active secret clearance within the last two years do not need to submit a SF 85P User Form. The contracting company will need to send a copy of the Letter of Consent (LOC) to the TMA Privacy Office for verification.

6.9. Notification Of Submittal And Termination

Contracting companies must notify the TMA Privacy Office when the security officer has submitted the SF 85P User Form 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 of the action, including the termination date.

6.10. Exception Or Extensions

Exceptions to or extensions beyond any end date or other requirement will be granted (if approved) only by the Director, TRICARE or the Deputy Director, TRICARE. Any exception or extension, if provided, will be in response to a written request, and based upon appropriate health program interests.

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

7.1. 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](#)).

7.2. Contractor Responsibilities

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

7.2.2. 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](#).

7.2.3. 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.

7.2.4. 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.

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

7.2.6. 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: NACLIC Team
Boyers, PA 16018

Routine Mail Delivery

U.S. Office of Personnel Management
P.O. Box 618
Attention: NACLIC Team
Boyers, PA 16018

7.2.7. 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.

7.2.8. 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.

7.2.9. 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.

7.2.10. For information on upgrading requests for trustworthiness determinations in process, see [paragraph 6.5.5.1](#).

8.0. PUBLIC KEY INFRASTRUCTURE (PKI)

8.1. 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.

8.2. 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.

8.2.1. 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.

8.2.2. 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.

8.2.3. 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]

8.2.4. 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.

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

8.4. 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.

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

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

8.5. 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

8.6. 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.

9.0. TELECOMMUNICATIONS

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

9.1.1. 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.

9.1.2. 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.

9.1.3. 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.

9.2. Contractor Provided IT Infrastructure

9.2.1. 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.

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

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

9.3. 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.

9.4. MHS Systems Telecommunications

9.4.1. 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.

9.4.2. 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.

9.4.3. 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.

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

9.4.5. 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.

9.5. Contractors Located On MTFs

9.5.1. 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.

9.5.2. 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.

9.5.3. 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.

9.5.4. 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.

9.6. DEERS

9.6.1. Primary Site

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

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

9.6.2. PCs/Hardware

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

9.7. TMA/TED

9.7.1. Primary Site

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

9.7.2. General

The common means of administrative communication between Government representatives and the contractor is via telephone and e-mail. An alternate method may be approved by TMA, as validated and authorized by TMA. Each contractor on the telecommunication network is responsible for furnishing to TMA at the start-up planning meeting (and update when a change occurs), the name, address, and telephone number of the person who will serve as the technical point of contact. Contractors shall also furnish a separate computer center (Help Desk) number to TMA which the TMA computer operator can use for resolution of problems related to data transmissions.

9.7.3. TED-Specific Data Communications Technical Requirements

9.7.3.1. Systems Interface Requirements

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

9.7.3.2. Communication Protocol Requirements

9.7.3.2.1. 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

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

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

9.7.3.2.4. "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.

9.7.3.2.5. File Naming Convention

9.7.3.2.5.1. 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.

9.7.3.2.5.2. 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.

9.7.3.2.5.3. 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.

9.7.3.2.5.4. 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.

9.8. TMA/MHS Referral And Authorization System

9.8.1. Primary Site

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

9.8.2. PCs/Hardware

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

9.9. TMA/TRICARE DCS

9.9.1. Primary Site

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

9.9.2. 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.)

FIGURES

Due to the size and nature of the first figure, [Figure 1-C-1](#) can be found on page 2.

TRICARE SYSTEMS MANUAL 7950.1-M, AUGUST 1, 2002

CHAPTER 1, ADDENDUM C

FIGURES

FIGURE 1-C-1 STANDARD FORM (SF) 85P SAMPLE

Standard Form 85P (EG) Revised September 1995 U.S. Office of Personnel Management 5 CFR Parts 731, 732, and 736		QUESTIONNAIRE FOR PUBLIC TRUST POSITIONS		Form approved: OMB No. 3206-0191 NSN 7540-01-317-7372 85-1602	
OPM USE ONLY		Codes		Case Number	
Agency Use Only (Complete items A through P using instructions provided by USOPM)					
A Type of Investigation	B Extra Coverage	C Sensitivity/Risk Level	D Compu./ADP	E Nature of Action Code	F Date of Action
G Geographic Location	H Position Code	I Position Title		Month	Day
J SON	K Location of Official Personnel Folder	None NPRC At SON	Other Address		Year
L SOI	M Location of Security Folder	None At SOI NPI	Other Address		ZIP Code
N OPAC-ALC Number	O Accounting Data and/or Agency Case Number				
P Requesting Official	Name and Title	Signature		Telephone Number	Date



In field P, format your response as follows:

**** COR Name, Title | COR Signature | COR Phone Number**

It is important to note field with an asterisk - this will alert OPM of the presence of inquiry contact information at the bottom of the page.

At the bottom of the page, note "***Inquiry Contact Information" and list the FSO Name, Title and Phone Number.

6 OTHER IDENTIFYING INFORMATION	Height (feet and inches)	Weight (pounds)	Hair Color	Eye Color	Sex (Mark one box)
7 TELEPHONE NUMBERS	Work (include Area Code and extension)		Home (include Area Code)		
8 CITIZENSHIP	I am a U.S. citizen or national by birth in the U.S. or U.S. territory/possession. Answer items b and d. I am a U.S. citizen, but I was NOT born in the U.S. Answer items b, c and d. I am not a U.S. citizen. Answer items b and e.			b Your Mother's Maiden Name	
9 UNITED STATES CITIZENSHIP	If you are a U.S. Citizen, but were not born in the U.S., provide information about one or more of the following proofs of your citizenship.				
Naturalization Certificate (Where were you naturalized?)					
City	State	Certificate Number	Month/Day/Year Issued		
Citizenship Certificate (Where was the certificate issued?)					
City	State	Certificate Number	Month/Day/Year Issued		
State Department Form 240 - Report of Birth Abroad of a Citizen of the United States					
Give the date the form was prepared and give an explanation if needed.	Month/Day/Year	Explanation			
U.S. Passport					
This may be either a current or previous U.S. Passport	Passport Number	Month/Day/Year Issued			
d DUAL CITIZENSHIP	If you are (or were) a dual citizen of the United States and another country, provide the name of that country in the space to the right.				
e ALIEN	If you are an alien, provide the following information:				
Place You Entered the United States:	City	State	Date You Entered U.S.	Alien Registration Number	Country(ies) of Citizenship
			Month Day Year		



**** Inquiry Contact Information: FSO Name, Title | FSO Phone Number.**

TRICARE SYSTEMS MANUAL 7950.1-M, AUGUST 1, 2002

CHAPTER 1, ADDENDUM C

FIGURES

FIGURE 1-C-2 SF 85P COVER SHEET INSTRUCTIONS

Part 1	Codes	Enter R for Advance Fingerprint Results
A	Type of Investigation	Depends on level of IT (ADP) applying for: <ul style="list-style-type: none"> IT (ADP) I - use code 30C IT (ADP) II - use code 08B
B	Extra Coverage	Enter 3 for Advance National Agency Check (NAC)
C	Sensitivity/Risk Level	Depends on level IT (ADP) applying for: <ul style="list-style-type: none"> IT (ADP) I - use code 6 (High Risk) IT (ADP) II - use code 5 (Moderate Risk)
D	Compu/ADP	Enter C if investigation is for an IT (ADP)-Computer position. If not, leave blank.
E	Nature of Action Code	Enter CON for contractor.
F	Date of Action	Leave blank.
G	Geographic Location	Leave blank.
H	Position Code	Leave blank.
I	Position Title	Enter CON for contractor.
J	SON	Enter 480G for TMA Privacy Office.
K	Location of Official Personnel Folder (OPF)	Check the correct box that gives the location of the OPF. <ul style="list-style-type: none"> NONE: If the person has never been a Federal employee. NPRC: If the OPF is at the National Personnel Records Center. AT SON: If the OPF is at the Submitting Office. OTHER ADDRESS: If the OPF is at any other location (for example, the SOI), give the address.
L	SOI	Enter DD03 .
M	Location of Security Folder	Check the correct box that identifies the location of the Security Folder. <ul style="list-style-type: none"> NONE: If there is no security file at your agency. AT SOI: If there is a security file at your agency, and it should be reviewed. NPI: If there is a security file at your agency, but it contains no pertinent information. OTHER ADDRESS: If your agency's security file should be reviewed and it is not at the SOI, furnish the address.
N	OPAC-ALC Number	Enter DoD-TMA .
O	Accounting Data and/or Agency Case Number	Enter the contracting company's SON .
P	Requesting Official	Enter the name, title, and signature of the contractor's facility security office, as well as the date and telephone number, including area code.

* FSO signature and telephone number should be put at the bottom of the SF 85P cover page.

FIGURE 1-C-3 COVER LETTER FOR FACILITY SECURITY OFFICER/PUBLIC TRUST OFFICIAL

Company Letterhead

From: Company Designated Official

To: Contracting Officer's Representative,
Contract #
Delivery Order #

Subject: Request for Signatures on SF 85P Questionnaire for Public Trust Positions

Attach is/are the Questionnaire for Public Trust Positions (SF 85P) form(s) for one/multiple employee(s) that needs to be processed for a background investigation. Please complete block P of each SF 85P form, sign this cover letter acknowledging receipt, and return this signed cover letter with the completed SF 85P forms. The following list contains the name(s), Social Security Number(s), date(s) of birth and ADP Level(s) requested for the attached SF 85P form(s). This cover letter must be scanned, encrypted, and e-mailed to Pamela Schmidt, Deputy Director, TMA Privacy Office at Pamela.Schmidt@tma.osd.mil. All investigation requests must be tracked in the Joint Personnel Adjudication System (JPAS) by the TMA Privacy Office staff.

Name	SSN	DOB	ADP Level Requested	Date
Doe, John F.	123-45-6789	6/15/1970	ADP-II	

John Smith
Designated Company Official

I, **(COR's Name)**, acknowledge receipt of the SF 85P form(s) for the personnel listed above. Received on **(Date)**. Completed and returned on **(Date)**.

Linda Smith
COR

TRICARE SYSTEMS MANUAL 7950.1-M, AUGUST 1, 2002

CHAPTER 2, SECTION 2.2

DATA REQUIREMENTS - DATA ELEMENT LAYOUT

4.0. PROVIDER FILE RECORD

ELN	ELEMENT NAME	FORMAT	POSITION	
			FROM	THRU
3-001	RECORD TYPE INDICATOR	X	1	1
3-005	PROVIDER TAXPAYER NUMBER	X(9)	2	10
3-010	PROVIDER SUB-IDENTIFIER	X(4)	11	14
3-015	PROVIDER TAXPAYER NUMBER IDENTIFIER	X	15	15
3-020	CONTRACTOR NUMBER	X(2)	16	17
3-025	PROVIDER CONTRACT AFFILIATION CODE	X	18	18
3-030	INSTITUTIONAL/NON-INSTITUTIONAL INDICATOR	X	19	19
3-035	PROVIDER NAME	X(40)	20	59
3-040	PROVIDER ADDRESS		60	119
3-045	PROVIDER STREET ADDRESS	X(30)	60	89
3-050	PROVIDER CITY	X(18)	90	107
3-055	PROVIDER STATE OR COUNTRY CODE	X(3)	108	110
3-060	PROVIDER ZIP CODE	X(9)	111	119
3-065	PROVIDER BILLING ADDRESS		120	179
3-070	PROVIDER BILLING STREET ADDRESS	X(30)	120	149
3-075	PROVIDER BILLING CITY	X(18)	150	167
3-080	PROVIDER BILLING STATE OR COUNTRY CODE	X(3)	168	170
3-085	PROVIDER BILLING ZIP CODE	X(9)	171	179
3-090	PROVIDER MAJOR SPECIALTY/TYPE OF INSTITUTION	X(10)	180	189
3-095	TYPE OF INSTITUTION TERM INDICATOR CODE	X	190	190
3-100	AMERICAN HOSPITAL ASSOCIATION ID NUMBER	X(9)	191	199
3-105	AHA MULTI-HOSPITAL SYSTEM CODE	X(4)	200	203
3-110	MEDICARE NUMBER	X(8)	204	211
3-115	PROVIDER ACCEPTANCE DATE	YYYYMMDD	212	219
3-120	PROVIDER TERMINATION DATE	YYYYMMDD	220	227
3-125	RURAL/URBAN INDICATOR	X	228	228
3-130	IDME RATIO	9V9(4)	229	233
3-135	IDME RATIO EFFECTIVE DATE	YYYYMMDD	234	241
3-140	AREA WAGE INDEX	9V9(4)	242	246
3-145	AREA WAGE INDEX EFFECTIVE DATE	YYYYMMDD	247	254
3-150	DRG EXEMPT/NONEXEMPT INDICATOR	X	255	255
3-155	DRG EXEMPT/NONEXEMPT EFFECTIVE DATE	YYYYMMDD	256	263
3-160	TRANSACTION CODE	X	264	264
3-165	RECORD EFFECTIVE DATE	YYYYMMDD	265	272
	FILLER	X(17)	273	289

5.0. TRANSMISSION RECORDS

5.1. The requirement for all electronic transmissions will incorporate the HIPAA mandated standards wherever feasible.

5.2. The first record in each transmission to TMA, whether by teleprocessing or magnetic tape, will be a transmission header, using the following format. Where value is specified under comments, the value must be reported exactly as shown.

TRANSMISSION HEADER RECORD FORMAT

POSITION(S)	DESCRIPTION	CONTENT	COMMENT
1-8	Alpha	Data Type	Must be "TED Data".
9-10	**	Delimiter	Must be **.
11-22	Alphanumeric	File Name	Must be named in accordance with Chapter 1, Section 1.1, paragraph 9.7.3.2.5.
23-24	**	Delimiter	Must be **
25-29	Alpha		Must be "FSIZE"
30-Variable	Numeric	File Size	Includes the total number of batch/voucher header records, provider, pricing and TED records (variable length). Includes transmission header, excludes transmission trailer.
Variable (2 positions)	**	Delimiter	Must be **.
Variable (6 positions)	Alpha	Record Type	Must be "RTYPEV".
Variable (2 positions)	**	Delimiter	Must be **.
Variable (7 positions)	Alpha		Must be "MAXRLN".
Variable	Numeric	Maximum Record Length	Length of the longest variable length record within the transmission. Must be > 0.
Variable (2 positions)	**	Delimiter	Must be **.
Variable - 80	Blank	Reserved	Must be HEX 40.

- Person repository
- National Enrollment Database (NED)
- Centralized CCDD repository
- PCM repository
- OHI repository
- SIT database

2.4. External Systems

All system to system interfaces to DEERS must use TCP/IP, FTP, HTTP, or HTTPS as specified by DEERS

- DEERS utilizes standard message protocols where appropriate
- DEERS defines the content and format of messages between DEERS and the MCSC
- DEERS and MCSC's and USFHP providers must utilize encryption for all messages that contain Privacy Act information
- DEERS specifies the method of encryption and authentication for all external interfaces (see [Chapter 1, Section 1.1, paragraph 9.4.](#), DEERS and MHS Telecommunications)
- All notifications are sent as full database images; they are not transaction-based. The MCSC must accept and apply the full image sent by DEERS. The MCSC or USFHP provider should add the information, if not present in their system. The MCSC or USFHP provider should update their system, if the information is present, by replacing their information with what is newly received from DEERS. Notifications are only intended to synchronize the most current information between DEERS and the MCSC. They do not synchronize history.
- DMDC centrally enforces all business rules for enrollment and enrollment-related events
- DEERS is the database of record for all eligibility and enrollment information

2.4.1. Data Sequencing

Since DEERS is tasked with resolving data conflicts from external systems using rules-based applications, the MCSC shall ensure proper data sequencing of transactions sent to DEERS. This aids in maintaining data validity and integrity.

