



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS

16401 EAST CENTRETECH PARKWAY
AURORA, COLORADO 80011-9066

TRICARE
MANAGEMENT ACTIVITY

PCSIB

CHANGE 7
7950.2-M
JUNE 4, 2009

**PUBLICATIONS SYSTEM CHANGE TRANSMITTAL
FOR
TRICARE SYSTEMS MANUAL (TSM)**

The TRICARE Management Activity has authorized the following addition(s)/revision(s) to 7950.2-M, issued February 2008.

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." This change brings this manual up-to-date with published Change 69 (November 5, 2008) to the Aug 2002 TRICARE Systems Manual 7950.1-M.

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

Jack Arendale
Chief, Purchased Care Systems
Integration Branch

ATTACHMENT(S): 26 PAGES
DISTRIBUTION: 7950.2-M

CHANGE 7
7950.2-M
JUNE 4, 2009

REMOVE PAGE(S)

CHAPTER 1

Table of Contents, page 1

Section 1.1, pages 11 through 25

★ ★ ★ ★ ★ ★

CHAPTER 2

Section 2.2, pages 9 and 10

INDEX

pages 1 and 2

INSERT PAGE(S)

Table of Contents, page 1

Section 1.1, pages 11 through 27

Addendum C, pages 1 through 4

Section 2.2, pages 9 and 10

pages 1 and 2

Chapter 1

General Automated Data Processing (ADP) Requirements

Section/Addendum	Subject/Addendum Title
1.1	General Automated Data Processing/Information Technology (ADP/IT) Requirements
1.2	Beneficiary Authentication Requirements
A	DoD 5200.2-R, January 1987 - AP6. Appendix 6
B	Federal Information Processing Standards (FIPS) Publication 140-2 - Security Requirements For Cryptographic Modules
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

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 1, Section 1.1

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

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

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

7.2 Formal Designations Required

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

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

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

7.3 Access Requirements

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

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

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

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

7.4 ADP/IT Category Guidance

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

7.4.1 ADP/IT-I - Critical Sensitive Position. A position where the individual is responsible for the development and administration of MHS IS/network security programs and the direction and control of risk analysis and/or threat assessment. The required investigation is equivalent to a Single-Scope Background Investigation (SSBI). Responsibilities include:

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

- Responsibility for the preparation or approval of data for input into a system, which does not necessarily involve personal access to the system, but with relatively high risk for effecting severe damage to persons, properties or systems, or realizing significant personal gain.
- Relatively high risk assignments associated with or directly involving the accounting, disbursement, or authorization for disbursement from systems of (1) dollar amounts of \$10 million per year or greater; (2) lesser amounts if the activities of the individuals are not subject to technical review by higher authority in the ADP/IT-I category to insure the integrity of the system.
- Positions involving major responsibility for the direction, planning, design, testing, maintenance, operation, monitoring and or management of systems hardware and software.
- Other positions as designated by the Designated Approving Authority (DAA) that involve a relatively high risk for causing severe damage to persons, property or systems, or potential for realizing a significant personal gain.

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

7.4.2.1 Other positions are designated by the DAA that involve a degree of access to a system that creates a significant potential for damage or personal gain less than that in ADP/IT-I positions. The required investigation for ADP/IT-II positions is equivalent to a National Agency Check with Law Enforcement and Credit Checks (NACLC).

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

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

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

7.5 Additional ADP/IT Level I Designation Guidance

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

7.5.1 Required Forms

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

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

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

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

7.5.3 Temporary Access (U.S. Citizens Only)

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

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

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

7.5.5 ADP/IT Level Trustworthiness Determination Upgrades

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

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

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

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

7.6 Access for Non-U.S. Citizens

7.6.1 Policy

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

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

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

7.7 Transfers Between TRICARE Contractor Organizations

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

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

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

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

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

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

7.8 New Contractor Personnel With Recent Secret Clearance

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

7.9 Notification Of Submittal And Termination

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

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

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

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

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

8.2 Contractor Responsibilities

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

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

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

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

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

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

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

Express Package Delivery

U.S. Office of Personnel Management
1137 Branchton Road
Attention: NAACL Team
Boyers, PA 16018

Routine Mail Delivery

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

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

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

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

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

8.3 Verification Process for Contractor Employees Requiring CACs

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

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

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

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

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

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

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

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

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

10.0 PUBLIC KEY INFRASTRUCTURE (PKI)

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

10.1 User Authentication

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

10.1.1 Process to Obtain a CAC

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

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

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

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

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

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

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

10.1.2 Initial Contract Start Up

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

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

10.1.3 Reverification

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

10.1.4 Lost or Damaged CACs

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

10.1.5 Termination of Employment

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

systems or networks.

10.1.6 Personal Identification Number (PIN) Resets

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

10.1.7 E-Mail Address Change

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

10.1.8 System Requirement for CAC Authentication

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

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

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

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

10.2 System Authentication

The contractor is required to obtain DoD acceptable PKI server certificates for identity and authentication of the servers upon direction of the CO. These interfaces include, but are not limited to, the following:

- Contractor systems for inquiries and responses with DEERS

- Contractor systems and the TED Processing Center

11.0 TELECOMMUNICATIONS

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

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

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

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

11.2 Contractor Provided IT Infrastructure

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

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

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

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

11.3.1 All contractors that use the DoD gateways to access government IT systems must submit the most current version of DD Form 2875 found on the DISA web site: <http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfo3211.html> in accordance with CO guidance. A DD Form 2875 is required for each contractor employee who will access any system on a DoD network. The DD Form 2875 must clearly specify the system name and justification for access to that system.

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

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

11.3.4 Contractors shall conduct a monthly review of all contractor employees who have been granted access to DoD IS/networks to verify that continued access is required. Contractors shall provide the TMA Privacy Office with a report of the findings of their review by the 10th day of the month following the review. Reports identifying changes to contractor employee access requirements shall include the name, SSN, Company, IS/network for which access is no longer required and the date access should be terminated.

11.4 MHS Systems Telecommunications

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

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

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

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

11.4.5 Maintenance and repair of contractor procured VPN equipment shall be the responsibility of the contractor. Troubleshooting of VPN equipment shall be the responsibility of the government.

11.5 Contractors Located On MTFs

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

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

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

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

11.6 TMA/TED

11.6.1 Primary Site

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

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

11.6.2 General

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

11.6.3 TED-Specific Data Communications Technical Requirements

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

11.6.3.1 Communication Protocol Requirements

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

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

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

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

11.6.3.1.4 "As Required" Transfers

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

11.6.3.1.5 File Naming Convention

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

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

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

11.6.3.1.6 Timing

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

11.6.3.1.6.1 Alternate Transmission

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

11.7 TMA/MHS Referral And Authorization System

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

11.8 TMA/TRICARE Duplicate Claims System

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

- END -

Figures

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

TRICARE Systems Manual 7950.2-M, February 1, 2008

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		ZIP Code		
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)
					<input type="checkbox"/> Female <input type="checkbox"/> Male
7 TELEPHONE NUMBERS	Work (include Area Code and extension)		Home (include Area Code)		
	Day	Night ()	Day	Night ()	
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.				b Your Mother's Maiden Name
a Mark the box at the right that reflects your current citizenship status, and follow its instructions.	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.				
c 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?)					
Court	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.				Country
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		

Exception to SF85, SF85P, SF85P-S, SF86, and SF86A approved by GSA September, 1995.
Designed using Perform Pro, WHS/DIOR, Sep 95



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

TRICARE Systems Manual 7950.2-M, February 1, 2008

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	06/15/1970	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

- END -

5.0 TRANSMISSION RECORDS

5.1 The requirement for all electronic transmissions will incorporate the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandated standards wherever feasible.

5.2 The first record in each transmission to TRICARE Management Activity (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 11.6.3.1.5.
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)	**	Delimitier	Must be **.
Variable (6 positions)	Alpha	Record Type	Must be "RTYPEV".
Variable (2 positions)	**	Delimiter	Must be **.
Variable (7 positions)	Alpha		Must be "MAXRLEN".
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.

5.3 Appended to the end of each transmission to TMA, whether by teleprocessing or magnetic tape, will be a transmission trailer record. The format for the transmission trailer record follows:

TRANSMISSION TRAILER RECORD FORMAT

POSITION(S)	DESCRIPTION	CONTENT	COMMENT
1	Alpha	Record ID	Must be "@" sign.
2-3	Alphanumeric	Contractor Number	TMA-assigned Contractor number.
4-10	Alphanumeric	Transmission Date	Enter in YYYYDDD format.
11-14	Numeric	Batch Count	Number of batches and/or vouchers in the transmission.

TRICARE Systems Manual 7950.2-M, February 1, 2008

Chapter 2, Section 2.2

Data Requirements - Data Element Layout

TRANSMISSION TRAILER RECORD FORMAT (CONTINUED)

POSITION(S)	DESCRIPTION	CONTENT	COMMENT
15-20	Numeric	Record Count	Includes the total number of batch/voucher header records, provider, pricing and variable length TED records. Excludes transmission header and transmission trailer.
21-80	Blank	Reserved	Must be HEX 40.

5.4 Transmissions will be returned to the contractor, with appropriate error codes appended, if any of the following occur:

ERROR CODE	ERROR TYPE	VALIDATION RULE
1200	Transmission header record not found	First record of the file must be a Transmission Header (first position is 'T').
1201	No records found in Transmission file	Byte count of the file = 0.
1202	Data Type is incorrect	Data Type must be "TED Data" - upper/lower case as shown is required. Cannot be all lower or all upper case.
1203	Second transmission header found	Second Transmission Header (first position is 'T') must not be found.
1207	Value of MAXRLEN in transmission header is not possible	MAXRLEN must be a valid value based on the combinations of record lengths included. Compare against all possible record lengths for Header (1), Inst (450), Non-Inst (99), and Provider (1) records.
1210	Transmission trailer record not found	A record must be found with first position = '@'.
1220	Second record is not a batch or voucher header record	Second record of the transmission must be batch/voucher record (record type = 0 or 5).
1240	Header record error in FSIZE, Record Type, or MAXRLEN fields)	'FSIZE', 'RTYPEV' and 'MAXRLEN' literals must be found in Transmission Header record and value of MAXRLEN must be > 0 and < 25535.
1250	Record type other than 0, 1, 2, 3, 4,5, T, or @ is invalid)	Record Type (first position of the record) must be 0, 1, 2, 3, 4, 5, 6, 9, T, or @.
1260	Extraneous data found after transmission trailer record	No record should be found after Trailer Record of the transmission file.
1290	Count of batch/voucher headers on trailer not equal headers read	Count of batch/voucher headers on trailer must match count of batch/vouchers.
1291	Batch/voucher Identifier code invalid	Batch/voucher identifier must be = 3, 4, or 5.
1295	Total record count on transmission trailer record not in balance.	Record count of transmission trailer must match total record count (except transmission header and trailer) of the file.
1296	Contractor number in trailer record does not match batch/voucher contract number	The contractor number (positions 2-3) in the transmission trailer record must correspond with the contractor number (ELN 0-010) in the batch/voucher header record(s) in the transmission file.
1299	Transmission header file-size not in possible in file	Transmission Header file size (FSIZE) must match total record count (except transmission header) of the file.
1998	Invalid non-printable character	Transmission file must not contain invalid non-printable characters (ASCII Values 0-9, 11-31, 127-255)

Index

A	Chap	Sec/Add
Acronyms And Abbreviations		Appendix A

B	Chap	Sec/Add
Beneficiary Authentication Requirements	1	1.2

D	Chap	Sec/Add
Data Reporting		
Provider File Record Submission	2	1.2
TRICARE Encounter Data Record Submission	2	1.1
Data Requirements		
Adjustment/Denial Reason Codes	2	G
Contract Area Of Responsibility	2	I
Country And/Or Island Codes	2	A
Data Element Layout	2	2.2
Default Values For Complete Claims Denials	2	M
Dependent Elements & Values For Rank Code, Sponsor Pay Category	2	K
Header Record Data	2	2.3
Health Care Delivery Program (HCDP) Plan Coverage Code Values	2	L
Institutional/Non-Institutional Record Data Elements		
A - D	2	2.4
E - L	2	2.5
M - O	2	2.6
P	2	2.7
Q - S	2	2.8
T - Z	2	2.9
Other Special Procedure Codes	2	E
Overview	2	2.1
Pay Plan Code Valid Values	2	J
Place Of Service/Type Of Service Allowable Relationships	2	F
Provider Major Specialty Codes	2	C
Provider Record Data	2	2.10
Revenue Codes	2	H
State Codes	2	B
Type Of Institution Codes	2	D
DEERS Concepts And Definitions	3	1.2
DEERS Functions	3	1.4
Defense Manpower Data Center (DMDC) Support	3	1.5

D (Continued)	Chap	Sec/Add
DoD 5200.2-R, January 1987 - AP6. Appendix 6	1	A

F	Chap	Sec/Add
Financial Edit Requirements	2	8.1
FIPS PUB 140-2 - Security Requirements For Cryptographic Modules	1	B

G	Chap	Sec/Add
General ADP/IT Requirements	1	1.1
Figures	1	C
General Edit Requirements Overview	2	3.1

H	Chap	Sec/Add
Header Edit Requirements		
ELN 000 - 099	2	4.1

I	Chap	Sec/Add
Institutional Edit Requirements		
ELN 000 - 099	2	5.1
ELN 100 - 199	2	5.2
ELN 200 - 299	2	5.3
ELN 300 - 399	2	5.4
ELN 400 - 499	2	5.5
Interface Overview	3	1.3

N	Chap	Sec/Add
Non-Availability Statement (NAS)	4	1.1
Non-Institutional Edit Requirements		
ELN 000 - 099	2	6.1
ELN 100 - 199	2	6.2
ELN 200 - 299	2	6.3
ELN 300 - 399	2	6.4

P	Chap	Sec/Add
Personnel Security Program	1	A
Provider Edit Requirements		
ELN 000 - 099	2	7.1
ELN 100 - 199	2	7.2

R	Chap	Sec/Add
Referenced Documents	3	1.1

TRICARE Systems Manual 7950.2-M, February 1, 2008

Index

S	Chap	Sec/Add
Standard Form (SF) 85P	1	1.1
Sample	1	C

T	Chap	Sec/Add
Test Environment	3	1.6

U	Chap	Sec/Add
UB-04/UB-92 Conversion Table - To Be Used For Reporting Non-Institutional TED Records	2	N