

ATTACHMENT D: ACCESS TO THE HA/TMA NETWORK/ DOD SYSTEMS

PERSONNEL SECURITY DIVISION ADP/IT REQUIREMENTS

Instructions for Contractor Access to DOD IT Systems
<http://tricare.mil/tma/aboutTMA/oa/psd/adpit.aspx>

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:

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:

dollar amounts of \$10 million per year or greater, or

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

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. The required investigation is equivalent to a National Agency Check with Law Enforcement and Credit (NACLC). Responsibilities include but is not limited to:

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.

Accounting, disbursement, or authorization for disbursement from systems of dollar amounts less than \$10 million per year.

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.

NOTE: 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 a SSBI. Investigations submitted before 2000 for a NAC (ADP/IT-II/III) will need to submit a new SF85P, Questionnaire for Public Trust Positions and FD 258 fingerprint card for an ADP/IT-III to be upgraded to an ADP/IT-II.

Procedure for Requesting ADP/IT-I

ALL TMA contracting companies requiring ADP/IT-I Trustworthiness Determinations for their personnel are required to submit a written request for approval to the Personnel Security Division (PSD). The justification will be submitted to: TMA PSD, Skyline 5, 5111 Leesburg Pike, Suite 810, Falls Church, VA

22041, on the contracting company's letterhead. The request letter must be signed by, at a minimum, by 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 ADP/IT-I. Contractors shall not apply for an ADP/IT-I (SSBI) investigation unless specifically authorized by PSD.

Questions & Answers

Why must contractors apply for IT (ADP) levels of trust?

The Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), and the DoD Health Information Privacy Regulation (DoD 6025.18-R) along with the DoD 5200.2R Personnel Security Program (January 1987), and the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) require that the DoD put in place appropriate safeguards to protect sensitive data. These safeguards against inappropriate use and disclosure must be upheld by contractors and others who have access to information systems containing protected health information. Background checks for all personnel who will obtain access to DoD IT systems holding sensitive but unclassified (SBU) data is one method of protection employed by DoD. SBU data is an informal designation for all information that, by law or regulation, requires some form of protection but is outside of a formal system for classifying national security information.

What are some examples of IT (ADP) positions that require levels of trust?

The following are typical category assignments for each IT specialty title defined in the OPM Position Classification Standard "Administrative Work in the Information Technology Group, GS-2200." Other IT-related positions should be categorized based on the particular set of duties and responsibilities of the position and the scope, and level of privileges authorized.

Security: IT-I (IT-II if primarily policy, planning or awareness focused)

Applications Software: IT-I or -II depending on specifics of application (IT-I if responsible for information security/information assurance applications)

Network Services: IT-I or IT-II (depending on the scope of network--as defined by criticality of or impact on Department or Federal government mission, geographic reach, and/or major or significant impact on other government agencies and/or the private sector--and level of privileges)

Systems Administration: IT-I (IT-II if stand-alone system or if the ability to compromise is limited to system/network operation)

Operating Systems: IT-II (IT-I if incumbent acts independently, without oversight/review)

Internet: IT-II (IT-I if privileged access to network functions)

Policy and Planning: IT-II if responsible for information security/information assurance program or if individual also has privileged access

Systems Analysis: IT-II if responsible for information security/information assurance systems

Data Management: IT-II if responsible for safeguarding sensitive data/information

Customer Support: IT-II (IT-I if privileged access; or IT-II if ability to set/change user access privileges (scope and level sensitive))

Other activities or specialties that may have significant IT duties include the following:

Computer Clerk and Assistant or Computer Operation: Typically IT-II, but may be higher if there is access to system/network control functions.

Computer Engineer: Generally hardware focused; typically IT-II, but specific categorization depends on function and application of the specific hardware/component (e.g., chip/board design may be IT-I), degree of supervision/review by higher authority, etc.

Criminal Investigating: Law enforcement activities associated with computer/network crime (e.g., forensic analysis; criminal investigation) – categorization depends upon required level of access (e.g., privileged/non-privileged).

Miscellaneous management and program analysis and other scientists, subject matter experts, and professionals: Depends upon required level of access (e.g., privileged/non-privileged)

Technical editors and other subject matter experts who develop Web pages, but whose primary expertise is not technical knowledge of Internet systems, services, and technologies: Categorize under "Internet" IT specialty; if non-privileged access, may be assigned IT-II designation

Miscellaneous IT specialists (As required by specifics of new technology/evolving specialty area): Use appropriate IT specialty

Threat and vulnerability assessment (e.g., red-teams; penetration testing): Determined by the purpose and scope of the assessment objective and required level of access

Certificate Management Authorities (CMA) to include Verifying Officials (VO): Typically IT-II, but may be higher if operating CMA equipment associated with Public Key Infrastructure operating above the DoD Class 4 assurance level.

What is the minimum ADP/IT requirement for access to a DoD IT system containing sensitive but unclassified data?

An ADP/IT-II (NACLC) is the minimum requirement for access to DoD IT Systems containing data for M2, MDR, PEPR, TDCS, Essence and all other MHS Accounts. Personnel accessing data associated with Data Use Agreements (DUAs) are also required to have an ADP/IT-II. An ADP/IT is a public trust position, not a security clearance. A Secret security clearance is acceptable in lieu of an ADP/IT-II. An ADP/IT trustworthiness determination is obtained by completing the following steps:

The contracting company Facility Security Officer (FSO) must complete the SF85P Agency Use Block (AUB) in e-QIP with the appropriate codes for a NACLC.

The contracting company FSO must initiate the applicant into e-QIP using the OF 306.

TRICARE contractors must complete the SF85P (Questionnaire for Position of Public Trust) in e-QIP and the FD258 (fingerprint card). The investigation covers a period of seven years.

Contractor personnel working in Military Treatment Facility's (MTF) should work with the facility security officer to submit the appropriate documents to obtain the NACLC investigation.

The contracting company FSO must notify the PSD upon the termination of contractor personnel on their contract.

ADP/IT Forms

Each contractor employee shall be required to complete and submit the necessary forms, fingerprint cards, and other documentation as may be required by OPM to open and complete investigations. Currently, contractors are required to complete and submit through the Electronic Questionnaire Investigations Processing (e-QIP), the OF 306, "Declaration of Federal Employment", the SF 85P, "Questionnaire for Public Trust", and the hard copy FD 258, Fingerprint card. 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 incomplete.

Managed Care Support Contractors are still authorized to submit the paper copy of the SF85P until required to use e-QIP. New managed care contracting support companies are still required to obtain a Submitting Office Number from OPM by submitting the PIPS Form 12.

NOTE: The appropriate TMA billing codes will be provided following contract award. The billing information will be contained in the SF85P Template for companies using e-QIP. New contracting companies should contact PSD to obtain the PIPS Form 12 when applying for a Submitting Office Number (SON). The new contracting company must provide the PSD with the TMA contract number, delivery order number, and the start and end date of the contract. The application and billing formation must be requested from PSD. Each contracting company or subcontracting company must contact the PSD individually for this information.

NOTE: Upon complete phase-in of e-QIP, contracting companies will no longer need to apply for a Submitting Office Number from OPM.

Foreign Nationals/(Non) US Citizens

DoD 5200.2-R, Personnel Security Program, dated January 1987, does not mention ADP/IT levels of trust for non-U.S. citizen contractor employees. As a result, in the past DoD offices did not follow one consistent procedure for ensuring that non-U.S. citizen contractor employees had received the appropriate background checks before gaining access to DoD information systems.

DoD policies state that the required investigation must be completed and favorably adjudicated prior to authorizing ADP/IT access to DoD systems/networks. Interim approvals are not authorized to non U. S. citizen contractor employees for access to DoD systems/networks. In communication with the Office of the Under Secretary of Defense for Intelligence (USDI), non-U.S. citizen contractor employees are not currently being adjudicated for Trustworthiness Determinations, and therefore not being approved for Trustworthiness positions.

As a result of this decision, Managed Care Support Contractors should not hire non U.S. citizen contractor employees for positions that require access to DoD systems or SBU information on a DoD system. To bring such an employee on under a TRICARE contract, and initiate the investigation process that will not be adjudicated, would not be fiscally prudent.

The Privacy Act of 1974, the Health Insurance Portability and Accountability Act (HIPAA), and the DoD Health Information Privacy Regulation (DoD 6025.18-R) along with the DoD 5200.2-R Personnel Security Program (January 1987) require that the DoD establish appropriate safeguards to protect sensitive data on a DoD system. These safeguards against inappropriate use and disclosure must be upheld by contractors and others who have access DoD systems containing protected health information and SBU information.

For further information on ADP/IT levels of trust, contact tma.psd@tma.osd.mil. PSD continues to work with the DoD Security Office and OPM to streamline and simplify this process.