Revised – November 2010

COMMERCE ACQUISITION MANUAL
1337.70

DEPARTMENT OF COMMERCE
PERSONNEL SECURITY REQUIREMENTS

COMMERCE ACQUISITION MANUAL
1337.70

Table of Contents

PERSONNEL SECURITY REQUIREMENTS

SECTION 1 – OVERVIEW

1.1 Background

Based on federal laws, regulations, directives, and policies, it is an inherent Government function for a federal agency to protect its facilities and their occupants from harm and its information from unauthorized disclosure. Therefore, non-employees who are granted official access to a federally controlled facility or permanent access to a federal information system shall be subject to specific security screening requirements similar to those imposed upon employees. Personnel security investigative requirements for access to a federally controlled facility or a federal information system are set forth in the "Department of Commerce *Manual of Security Policies and Procedures"* and Department of Commerce Information Technology Security Program Policy (ITSPP), January 2009*.*

1.2 Purpose

The purpose of this Commerce Acquisition Manual (CAM) chapter is to establish procedures for adhering to personnel security processing requirements for contractors performing services on or within a Department of Commerce (DOC, Department) facility or through an Information Technology (IT) system, as required by the *Manual of Security Policies and Procedures* and ITSPP.

1.3 Applicability

This policy is applicable to Department of Commerce solicitations and contracts that meet all the following criteria:

a. Services,

b. Involving access to sensitive non-National Security or National Security Information, and

c. Performed on or within government facilities or through a DOC network or system.

1.4 Policy

All DOC service contracts that meet the criteria as stated in Section 1.3, are required to be designated by risk for non-National Security contracts and by sensitivity for National Security contracts. Guidance for risk designation, and specific background investigation requirements are outlined in Sections 2 and 3, respectively. The procedures contained herein implement the requirements of the DOC *Manual of Security Policies and Procedures* for requesting and processing personnel security background investigations.

END OF SECTION 1

SECTION 2 – RISK DESIGNATIONS AND SENSITIVITY LEVELS

2.1 Background

The contract designation is determined by evaluating the risk or sensitivity of the work being planned; the risk or sensitivity of the facility upon or in which the work is to be performed; the security impact level of the IT system to which personnel have access; the level of access privileges to an IT system; whether the contracted activities are to be performed during or outside of normal business hours; and the extent that a Government escort will be both necessary and available to the contract employees present in the facility or while IT access is required. The contract designation also determines the security/suitability requirements for the contract personnel who will perform the work. The costs for conducting the applicable security/suitability background checks are to be absorbed by the program office sponsoring the procurement.

The risk or sensitivity level designation shall be made by the program office representative (typically the assigned Contracting Officer Representative), in conjunction with Operating Unit management, cognizant security office, cognizant IT Security Officer, and the procurement office representative. The Contracting Officer Representative (COR) will review the work to be performed under the contract and assign the highest risk designation to the entire contract in accordance with the criteria stated below. The rationale for the designated risk level shall be documented and placed in the official contract file. Accordingly, each contract employee will undergo investigative processing based on the contract's risk level designation (see Chapters 10 and 11 of the DOC *Manual of Security Policies and Procedures*).

2.2 Non-IT Service Contracts (non-National Security)

The following risk designations should be used for Non-IT Service Contracts:

2.2.1 High Risk

A contract will be designated "High Risk" if it meets all the following criteria:

a. Work requiring continuous foreign travel of 90 days or more at any time during the performance of the contract under the auspices of the Department;

b. Work involving functions or operations of the Department that are critical to the accomplishment of the mission of the Department;

c. Work involving investigative, compliance, or senior-level auditing duties;

d. Work involving fiduciary, public contact, or other duties involving the highest degree of public trust; and

e. Any other work designated High Risk by the head of Operating Unit or departmental office.

2.2.2 Moderate Risk

A contract will be designated "Moderate Risk" if it meets the following criteria:

a. Work involving free access and movement during normal work hours within a Department of Commerce facility which houses National Security information or

equipment with little or no supervision by an appropriately cleared Federal Government employee;

b. Work occurring during restricted hours within a Department of Commerce facility which houses classified or sensitive information or equipment even though supervised by a Federal Government employee;

c. Work requiring access to sensitive information (information protected under the Privacy Act or Title 13 of the U.S. Code); or

d. Work involving foreign travel less than 90 days duration.

2.2.3 Low Risk

Work that does not fall into any of the categories noted above will be given a "Low Risk" designation.

2.3 IT Service Contracts (non-National Security)

Contract employees, regardless of appointment duration, requiring assignment of a system or network account for access to internal (i.e. non-public) Department of Commerce IT systems that do not require access to National Security information must undergo a background check based on consideration for the highest security categorization of the system(s) to which access is required and the access privileges required. A risk-based, cost effective approach must be followed to determine the risk of harm to the system in comparison to the opportunity for personnel to cause harm.

The following examples demonstrate the opportunity for personnel to cause harm depending on their access privileges, which impact the contract risk designation. The following examples are not all-inclusive, and CORs should contact their servicing IT Security Officer for additional assistance. Additional criteria for IT service contracts are described in DOC *ITSPP,* Sec. 4.13.2.

2.3.1 High Risk

Personnel with IT security authority, "root" access to systems, or access to software source code have opportunity to bypass system security control settings – for example, network/system administrator, system developer, and IT security program positions (such as IT Security Officer staff) or access to an email server or contents of multiple user's email accounts.

"Super-users" of High- or Moderate-impact systems who may modify core data stores, users with authority to electronically approve financial transactions, or users with access to personal/Privacy Act/other protected data (e.g. social security numbers in human resource systems, etc.) other than their own. For these types of access privileges, the risk designation depends on the security categorization of the system(s) involved. The potential impact of loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on operations, organizational assets, or individuals.

2.3.2 Moderate Risk

Account types with elevated, limited access rights typically provided to supervisors or users who review and modify data for others but do not have root-level access to systems or database administrator functions to directly access, modify, or delete data

from a database. The potential impact of the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on operations, organizational assets, or individuals.

2.3.3 Low Risk

Users with access to a DOC local area network, personal email, basic office applications (such as Microsoft Office), and personal data records (i.e. only personal/private information pertaining to themselves such as their personal time and attendance record). For these types of access privileges, the potential impact of the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

2.4 National Security Contracts

National Security work designated "special sensitive," "critical sensitive," or "non-critical sensitive" will determine the level of clearance required for personnel working on the contract. Personnel security clearances for National Security contracts in the Department of Commerce are processed according to the Department of Defense *National Industrial Security Program Operating Manual (NISPOM).* For additional guidance on National Security contracts, refer to Chapter 37, Industrial Security, of the DOC *Manual of Security Policies and Procedures.*

All contractor employee positions in DOC require a risk designation. In addition, contract personnel requiring access to National Security information must also have a sensitivity designation. The level of investigation required for a position is determined by its risk or sensitivity designation. The level of investigation required by the sensitivity designation will normally take precedence over that required by the risk designation. The exception to this requirement would be the investigation for a High Risk position requiring access to National Security information at the Secret level. Guidance for the designation of sensitive positions is outlined below.

2.4.1 Special Sensitive

Any position that the Head of an Operating Unit determines to be designated at a level higher than Critical-Sensitive. This may be due to special requirements under an authority other than Executive Order 10450 and 12968 (such as Intelligence Community Directive (ICD) 704.2 that sets investigative requirements and standards for access to Sensitive Compartmented Information (SCI) and other intelligence-related Special Sensitive information).

2.4.2 Critical Sensitive

Positions that have potential for exceptionally grave damage to the National Security. These positions may include access to Top Secret defense information; development or approval of war plans, plans or particulars of future, major, or special operations of war, or critical and extremely important items of war; investigative duties, the issuance of personnel security clearances, or other positions related to National Security, regardless of duties that require the same degree of trust.

2.4.3 Non-critical Sensitive

Positions that have the potential for serious damage to the National Security. These positions involve either access to Secret or Confidential National Security information or materials or to duties that may adversely affect, directly or indirectly, the National Security operations of the Department.

END OF SECTION 2

SECTION 3 – BACKGROUND INVESTIGATIONS AND SECURITY PROCESSING REQUIREMENTS

3.1 Background

The risk designation or sensitivity level of a contract determines the type of background investigation that will be conducted for the individual performing the work. These investigations provide an assessment of the suitability of an individual to protect the efficiency or integrity of Departmental operations or the national security, so that the individual may not pose a risk to Departmental activities and operations. Regardless of risk or sensitivity of the contract, requirements for Personal Identity Verification (PIV) under Homeland Security Presidential Directive-12 (HSPD-12) may dictate a more stringent background investigation for individuals performing work on the contract, especially for Low or non-IT Moderate Risk contracts.

3.2 Non-IT Service Contracts (non-National Security)

Contract employees requiring routine access to DOC facilities in order to perform work on non-IT DOC service contracts that do not require access to National Security information must undergo a background check based on the risk level of the contract.

Copies of the appropriate forms can be obtained from the COR or the Office of Security (OSY). Upon receipt of the required forms, the Contracting Officer Representative will forward the forms to the servicing Security Officer. The Security Officer will process the forms and advise the COR whether work can commence prior to the completion of the suitability determination based on the type of work and risk to the facility (i.e. adequate controls and restrictions are in place). The Contracting Officer Representative will notify the Contractor of an approved contract start date as well as favorable or unfavorable findings of the suitability determinations.

3.2.1 High Risk – Non-IT Services Contracts

A. Investigative Requirements – All contractor (and subcontractor) personnel proposed to be employed under a non-IT High Risk contract shall undergo a Background Investigation (BI) which should be updated every five (5) years.

B. Processing Requirements – The contractor must complete and submit the following forms to the Contracting Officer Representative:

   i. Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;

   ii. Form FD-258, Fingerprint Card with Office of Personnel Management's (OPM) designation in the ORI Block; and

   iii. Credit Release Authorization.

C. The COR will review these forms for completeness, initiate the CD-254, Contract Security Classification Specification, and forward the documents to the cognizant Security Officer. Upon completion of the security processing, the Office of Security, through the servicing Security Officer and the COR, will notify the Contractor in writing of the individual's eligibility to be given access to a DOC facility or DOC IT system.

3.2.2 Moderate Risk – Non-IT Service Contracts

A. Investigative Requirements – All contractor (and subcontractor) personnel proposed to be employed under a non-IT Moderate Risk contract shall undergo a Minimum Background Investigation (MBI) which should be updated every ten (10) years.

B. Security Processing Requirement – The contractor must complete and submit the following forms to the Contracting Officer Representative:

   i. Standard Form 85P, Questionnaire for Public Trust Positions;

   ii. Form FD-258, Fingerprint Card with OPM's designation in the ORI Block; and

   iii. Credit Release Authorization.

C. The Contracting Officer Representative will review these forms for completeness, initiate the CD-254, Contract Security Classification Specification, and forward the documents to the cognizant Security Officer. Upon completion of the security processing, the Office of Security, through the servicing Security Officer and the COR, will notify the Contractor in writing of the individual's eligibility to be given access to a DOC facility or DOC IT system.

   Security processing shall consist of limited personal background inquiries pertaining to verification of name, physical description, marital status, present and former residences, education, employment history, criminal record, personal references, medical fitness, fingerprint classification, and other pertinent information. For non-U.S. Citizens, the COR must request a Customs and Immigration Service (CIS), agency check. It is the option of the Office of Security to repeat the security processing on any contract employee at its discretion.

3.2.3 Low Risk – Non-IT Service Contracts

A. Investigative Requirements – Each person employed under a non-IT Low Risk contract shall undergo security processing by the Department's Office of Security as indicated below:

   i. Contractors requiring access to a DOC facility for more than 180 days are required to have a National Agency Check with Written Inquiries (NACI). The COR will forward a completed Standard Form 85 (SF-85), Questionnaire for Non-Sensitive Positions; Form FD-258, Fingerprint Card; and Credit Release Authorization to the servicing Security Officer within 3 business days from start of work, who will send the investigative packet to OPM.

   ii. Contractors requiring access to a DOC facility for less than 180 days shall have a Special Agreement Check (SAC) – Office of Federal Investigations (OFI) Form 86C (OFI-86C), as determined by DOC *Manual of Security Policies and Procedures*, Chapter 11. The COR will forward a completed OFI-86C, FD-258, Fingerprint Card, and Credit Release Authorization to OPM for processing. The scope of the SAC will include checks of the Security/Suitability Investigations Index (SII), other agency files (INVA), Defense Clearance Investigations Index (DCII), FBI Fingerprint (FBIF), and the FBI Information

Management Division (FBIN). In addition, for those individuals who are not U.S. Citizens (lawful Permanent Residents), the COR must request a CIS check on the SAC Form OFI-86C, by checking Block 7, Item I. In Block 13, the COR should enter the employee's Alien Registration Receipt Card number to aid in verification.

Any contract employee with a favorable SAC who remains on the contract over 180 days will be required to have a NACI conducted to continue working on the job site. The COR/Program Officer shall contact the cognizant security office if the duration of the contract will be extended beyond a 180-day period.

3.3 IT Service Contracts (non-National Security)

Individuals employed in High Risk positions, or Moderate Risk positions in the IT occupation, and those at the Moderate Risk level with "global access" to an automated information system, shall be subject to reinvestigation as deemed necessary, but not less frequently than once every five years.

3.3.1 High Risk – IT Service Contracts

A. Investigative Requirement – All contractor (and subcontractor) personnel proposed to be employed under an IT High Risk contract shall undergo a background investigation.

B. Security Processing Requirement – The contractor must complete and submit the following forms to the Contracting Officer Representative:

   i. Standard Form 85P, Questionnaire for Public Trust Positions;

   ii. Form FD-258, Fingerprint Card with OPM's designation in the ORI Block; and

   iii. Credit Release Authorization.

C. The COR will review these forms for completeness, initiate the CD-254, Contract Security Classification Specification, and forward the documents to the cognizant Security Officer. Upon completion of the security processing, the Office of Security, through the servicing Security Officer and the COR, will notify the Contractor in writing of the individual's eligibility to be given access to a DOC facility or DOC IT system.

3.3.2 Moderate Risk – IT Service Contracts

A. Investigative Requirement – All contractor (and subcontractor) personnel proposed to be employed under an IT Moderate Risk contract shall undergo a background investigation.

B. Security Processing Requirement – The contractor must complete and submit the following forms to the Contracting Officer Representative:

   i. Standard Form 85P, Questionnaire for Public Trust Positions;

   ii. Form FD-258, Fingerprint Card with OPM's designation in the ORI Block; and

iii. Credit Release Authorization.

C. The COR will review these forms for completeness, initiate the CD-254, Contract Security Classification Specification, and forward the documents to the cognizant Security Officer. Upon completion of the security processing, the Office of Security, through the servicing Security Officer and the COR, will notify the Contractor in writing of the individual's eligibility to be given access to a DOC facility or DOC IT system.

3.3.3 Low Risk – IT Service Contracts

A. Investigative Requirements – Each contractor employed in Low Risk IT service contracts will require a NACI to be processed.

B. Security Processing Requirements – The COR will forward a completed Form SF-85, Form FD-258, Fingerprint Card, and Credit Release Authorization to the servicing Security Officer within three business days from start of work, who will send the investigative packet to OPM. Individuals who are not U.S. Citizens (lawful Permanent Residents) must undergo a NACI that includes an agency check conducted by the Immigration and Customs Enforcement (ICE). The COR must request the ICE check as a part of the NACI.

3.4 National Security Contracts

3.4.1 Risk Assessment

Before requesting background investigations for personnel performing work on a national security contract, risk assessments must be conducted on all functions that are performed under the contract to determine the level of classification required for access to the National Security information. The Contracting Officer and COR must determine the level of sensitivity or security risk with the assistance of the servicing Security Officer. The sensitivity level of the contract then determines the type of background investigation required for contract employees to perform work on the contract. In addition, the Contracting Officer must obtain verification through Office of Security that the contractor has been granted a facility security clearance from the Defense Industrial Security Clearance Office (DISCO) prior to the release of any National Security information to a Contractor. See Chapter 37, Industrial Security, of the DOC *Manual of Security Policies and Procedures* for a description of this process.

3.4.2 Investigation Requirements

National Security contracts require employed contractors to gain access to National Security information in the performance of their work. Regardless of the contractors, consultant, or expert's location, appropriate security access and fulfillment of cleared facility requirements as determined by the NISPOM must be met. All contractors, consultants, and experts are subject to the appropriate investigations indicated below and are granted appropriate security access by the Office of Security based on favorable results.

All employees on Special or Critical Sensitive contracts require an updated personnel security background investigation every five years. Employees on Non-Critical Sensitive contracts will require an updated personnel security background investigation every ten years.

3.4.3 Additional Considerations for National Security Contracts

Only U.S. Citizens are eligible to obtain a security clearance. Security clearances for personnel performing work on a National Security contract must be granted by DISCO through the NISPOM process. Guidelines for initiating the investigations are provided in Chapter 11 of the DOC *Manual of Security Policies and Procedures*. On a case-by-case basis, the Office of Security may grant individual contactors a security clearance for the performance of short-term National Security work. Information on processing this request is contained in Chapter 12 of the *Manual of Security Policies and Procedures,* Access to National Security Information.

No National Security materials or documents shall be removed from a DOC facility. The circumstances of the work performance must allow DOC to retain control over the information and keep the number of contract personnel with access to a minimum.

END OF SECTION 3

SECTION 4 – FOREIGN NATIONALS (NON- U.S.CITIZENS)

4.1 Background

Every effort shall be made to ensure that non-U.S. Citizens are not employed in duties that may require access to National Security information. However, compelling reasons may exist to grant access to National Security information to an Immigrant Alien or a Foreign National. Such individuals may be granted a Limited Access Authorization in those rare circumstances where the non-U.S. Citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific U.S. Government contract involving access to specified National Security information and a cleared or clearable U.S. Citizen is not readily available.

The Limited Access Authorization may only be issued through the NISPOM process. With the concurrence of the Director for Security in instances of special expertise and with the concurrence of the Department of Defense in furtherance of U.S. Government obligations pursuant to U.S. law, treaty, or international agreements. Foreign National Guests who will have access to Departmental facilities for more than three (3) days will be subject to a security check at the discretion of the Director of Security. Additional criteria for non-U.S. Citizens are described in the DOC *Manual of Security Policies and Procedures,* Chapter 11.

Permanent Resident must provide proof of permanent residency status thirty (30) working days prior to their visit. Foreign Nationals claiming refugee status or asylum will continue to be governed by the policies outlined in Chapter 11 of DOC *Manual of Security Policies and Procedures* and Department Administrative Order (DAO) 207-12, Foreign National Visitor and Guest Access Program*,* until such times as their cases have been properly adjudicated under the Immigration and Naturalization Act (8 U.S.C. 1157 and 1158, respectively).

Policy and guidance for Foreign National Visitor and Guests Access to Departmental Facilities and Activities is outline in Department Administrative Order 207-12, Foreign National Visitor and Guest Access Program.

END OF SECTION 4

SECTION 5 – CONTRACT REQUIREMENTS AND PROCEDURES

5.1 Solicitations/Contract Language

All solicitations/contracts that meet the criteria in Section 1.3 are required to contain language regarding the risk or sensitivity position designation and the associated security requirements. It is recommended that the COR, Operating Unit management representative and cognizant Security Officer work with the Contracting Officer to tailor the provisions to the particular situation. The rationale for the designed risk level shall be documented and placed in the official contract file.

The Contracting Officer shall insert the applicable Commerce Acquisition Regulation (CAR) clause(s) in service solicitations and contracts:

a. CAR clause 1352.237-70, which contains contract language for Security Processing Requirements for High or Moderate Risk contracts;

b. CAR clause 1352.237-71, which contains contract language for Security Processing Requirements for Low Risk contracts;

c. CAR clause 1352.237-72, which contains contract language for Security Processing Requirements for National Security contracts;

d. CAR clause 1352.237-73, which contains contract language for Foreign Visitor and Guest Access to Departmental resources; and

e. CAR clause 1352.239-72, which contains contract language for Security Requirements for IT resources.

5.2 Requesting Background Investigations

Once an award is made, the COR as a PIV sponsor, is responsible for following procedures for the PIV credential process as specified at the Office of Security website at: http://www.osec.doc.gov/osy/HSPD-12/HSPD-12Information.html. Work may not commence until the contract employees have been granted eligibility for access to a DOC facility or IT system. There are differences in the timing of the form submittal requirements as well as differences in whether a proposed contract employee can begin work prior to being determined suitable. Specific information on the timing of form submittals and work commencement can be found in the *Manual of Security Policies and Procedures.*

5.3 Notifications of Results

The Office of Security will conduct the required background checks as determined by the DOC *Manual of Security Policies and Procedures,* Chapter 11, and will provide notification of the results (both favorable and unfavorable findings) in writing to the COR.

Any information contained in the contract file pertaining to the background investigation, including the specific notification of the results of the completed background investigation, shall not be released to anyone by the Contracting Officer or the COR. When the notification of the results of the background investigation is no longer required by the COR, it should be destroyed by approved methods. See Section 4.10.4 of the DOC *IT Security Program Policy* for more information on approved methods that may be applied to both paper and electronic media.

5.3.1 Favorable Findings

Favorable findings shall be forwarded to the Contractor by the COR. The COR shall provide a copy of the written favorable designation to the Contracting Officer.

5.3.2 Unfavorable Findings

For unfavorable or questionable findings, the COR, in coordination with the Contracting Officer and cognizant Security Officer, shall seek the advice of legal counsel in determining the appropriate course of action. The determined course of action shall reflect the duly considered options of the Government parties, and priority shall be given to the overall objective of protecting Government personnel and facilities.

The notification of the results that a given employee does not meet the suitability or sensitivity requirements for the contract, or that further information is needed, shall be made in writing by the CO directly to the Contractor. The notification shall consider the requirements of the Privacy Act and other laws and regulations concerning privacy information, and shall include the request, if applicable, that another candidate be proposed as soon as possible. Upon the advice of legal counsel, appropriate reference may be made to the release from liability that was submitted as part of the initial suitability determination package. A copy of the notification of the results of the background investigation shall be maintained in the contract file, although all specific information concerning the subject shall be retained in the cognizant facility Security Officer's files in accordance with the Privacy Act and other applicable laws and regulations. In all cases, the standards and procedures applied to contractor employees shall be comparable to those applied to Government employees.

END OF SECTION 5

END OF CAM 1337.70

APPENDIX A
Definitions

Contracting Official – Individuals with specific authority to process and recommend or specifically obligate the Government; includes Purchasing Agents, Contract Specialists and Contracting Officers (CO) (including Program Officials with Delegated Procurement Authority).

Contracting Officer Representative (COR) – A Federal employee delegated limited authority by a Contracting Officer to monitor and perform specific, enumerated contract management duties related to contract planning, contract administration, technical oversight, and closeout to ensure that contractor's performance meets the standards set forth in the contract. Contracting Officer Representatives may be designated as Point of Contact/Order Contact (P/OC), Contracting Officer Technical Representative (COTR), or a Task Manager (TM).

Foreign National (FNs) – Any non-US Citizen or 'Permanent Resident' (defined by the US Citizenship and Immigration Services as "[a]ny person not a citizen of the US who is residing in the US under legally recognized and lawfully recorded permanent residence as an immigrant." Also known as "Permanent Resident Alien," "Lawful Permanent Resident," "Resident Alien Permit Holder," or "Green Card Holder").

Foreign National Visitor – Any Foreign National who is accessing Departmental facilities for three (3) or fewer days or attending a conference of five (5) or fewer days. Attendance at the conference must be specified as the purpose for the visit and must include the dates of the conference.

Foreign National Guest – Any Foreign National who will be accessing Departmental facilities for more than three days.

Information Technology – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources (Clinger Cohen Act of 1996, Section 5002).

National Security – The national defense or foreign relations of the United States (refer to Executive Order 13526).

IT Security Program Manager – Responsible for developing and maintaining an Operating Unit, Bureau, or organization's IT security program.

Servicing Security Office – A field office of the Office of Security that provides security services, support, and guidance to DOC organizations. A servicing security office may provide services and support to a single Bureau or to all DOC organizations in a given geographical area.