Revised – October 2015

COMMERCE ACQUISITION MANUAL
1337.70

DEPARTMENT OF COMMERCE
PERSONNEL SECURITY REQUIREMENTS

COMMERCE ACQUISITION MANUAL
1337.70

Table of Contents

SECTION 1 – OVERVIEW 1
1.1 BACKGROUND 1
1.2 PURPOSE 1
1.3 APPLICABILITY 1
1.4 POLICY 1

SECTION 2 – RISK DESIGNATIONS AND SENSITIVITY LEVELS 3

2.1 BACKGROUND 3
2.2 SERVICE CONTRACTS (NON-NATIONAL SECURITY) 3
2.3 CLASSIFIED CONTRACTS (NATIONAL SECURITY) 4

SECTION 3 – BACKGROUND INVESTIGATIONS AND SECURITY PROCESSING REQUIREMENTS 6

3.1 BACKGROUND 6
3.2 HSPD12 REQUIREMENTS 6
3.3 SERVICE CONTRACTS (NON-NATIONAL SECURITY) 6
3.4 CLASSIFIED CONTRACTS (NATIONAL SECURITY) 10

SECTION 4 – FOREIGN NATIONALS (NON- U.S. CITIZENS) 11

SECTION 5 – CONTRACT REQUIREMENTS AND PROCEDURES 12

5.1 SOLICITATIONS/CONTRACT LANGUAGE 12
5.2 REQUESTING BACKGROUND INVESTIGATIONS 12
5.3 NOTICATION OF RESULTS 12

APPENDIX A -DEFINITIONS A-1

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, contractor personnel 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 federal 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*, December 2012 and the *Department of Commerce Information Technology Security Program Policy (ITSPP)*, September 2014.

1.2 Purpose

The purpose of this Commerce Acquisition Manual (CAM) chapter is to implement revised procedures for adhering to personnel security processing requirements for contractor personnel performing services on or within a Department of Commerce (DOC, Department) facility or through an Information Technology (IT) system.

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 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 Department of Commerce service contracts that meet the criteria 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 contract designation, and specific background investigation requirements are outlined in Sections 2 and 3, respectively. The procedures contained herein implement the requirements of the *Department of Commerce 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, and 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/fitness requirements for the contract personnel who will perform the work. The costs for conducting the applicable security/fitness background checks are to be absorbed by the program office sponsoring the procurement.

The program office representative (typically the Contracting Officer Representative (COR)) shall review the work to be performed and consult with the Program Office management, Information Technology (IT) Security Officer, Servicing Security Officer, and/or the procurement office representative to determine the appropriate risk and sensitivity level designation. The program office representative shall assign the highest risk or sensitivity designation to the entire contract, in accordance with the criteria in Sections 2.2 and 2.3, and document the designation in the acquisition planning documents and the Security Requirements section of the Statement of Work. The rationale for the designated risk level shall be documented and placed in the contract file. Contractor personnel assigned to the contract will undergo investigative processing based on the contract risk and/or sensitivity level designation (see Chapters 10 and 11 of the *Department of Commerce Manual of Security Policies and Procedures*).

2.2 Service Contracts (non-National Security)

The following risk designations shall be used for all service contracts. When considering the risk level of contracts, program offices shall consider the risk levels associated with comparable federal government positions, determined by the Office of Personnel Management (OPM) Automated Position Designation Tool:

2.2.1 High Risk

A contract shall be designated "high risk" if it meets the criteria, as determined by the OPM tool. However, some examples of duties and functions that may rise to the level of "high risk" could include:

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

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. Work involving automatic information networks and/or systems functions such as:

    i. Plan, direct, and implement a computer security program.

ii. Plan, design, direct, and administer a computer system (IT hardware, software, and/or data communications) capable of processing and storing new sensitive or classified information, without affecting the IT security categorization impact level or the National Security Information (NSI) sensitivity classification of the information stored on the system.

iii. Access to a computer system, during the operation or maintenance process that could result in grave damage to that computer system or in personal gain when there is no possible access to classified information.

f. Any other work designated "high risk" by the head of the Operating Unit or departmental office.

2.2.2 Moderate Risk

A contract shall be designated "moderate risk" if it meets the criteria as determined by the OPM tool. However, some examples of duties and functions that may rise to the level of "moderate risk" could include:

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; Title 13 of the U.S. Code); or data with a similar designation level (e.g. Federal Information Processing Standards Publications (FIPS PUB199));

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

e. Work in which a contractor is responsible for the direction, planning, design, operation access/use, or maintenance of a computer system, and whose work is technically reviewed by Federal Government personnel whose position sensitivity is critical sensitive or above to ensure the integrity of the system.

2.2.3 Low Risk

A contract shall be designated as "low risk", if it does not meet any of the criteria for "high risk" (Section 2.2.1) or "moderate risk" (Section 2.2.2) due to lower risk factors.

2.3 Classified Contracts (National Security)

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 *Department of Commerce Manual of Security Policies and Procedures.*

All contractor employee positions in DOC require an initial risk determination. 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.

2.3.1 Special Sensitive
Positions determined by the Head of an Operating Unit to be a level above 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).

2.3.2 Critical Sensitive
Positions requiring access up to and including Top Secret information with the potential to cause exceptionally grave damage to National Security.

2.3.3 Non-critical Sensitive
Positions requiring access up to and including Secret or Confidential National Security information or materials or duties with the potential for serious damage, directly or indirectly, to National Security.

END OF SECTION 2

SECTION 3 – BACKGROUND INVESTIGATIONS AND SECURITY PROCESSING REQUIREMENTS

3.1 Background

The risk or sensitivity designation of a contract determines the type of background investigation that will be conducted for the individual performing the work. These investigations assess individual fitness of an individual to protect the efficiency or integrity of Departmental operations or the national security to lessen the risk to Departmental activities and operations. For "low risk or "moderate risk" contracts, 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 contracts.

3.2 HSPD-12 Requirements

The program office representative (typically the COR) shall consult with building security, IT Security, and Personnel Security to determine if access to DOC information technology, sensitive data, regular or prolonged access to DOC-controlled facilities, or any combination of these three is required. If required, the risk level, security, access, identification, and sensitivity level(s) for the position(s) and the work to be performed will be assessed and the results documented in the acquisition planning documents.

A PIV sponsor, typically the COR but may be a Bureau Security Contact, Servicing Security Officer, and/or other individual as determined by the supervisor and manager of the respective program, will be assigned to assist contractor personnel during the initial vetting and credentialing process, and when credentials are renewed or rescinded. In order to facilitate the PIV credential process, the PIV sponsor shall submit a copy of applicable HSPD-12 documents to their respective Servicing Security Office within five (5) business days after award. Procedures for sponsorship are specified at the Office of Security (OSY) website: http://www.osec.doc.gov/osy/hspd-12/HSPD-12Information.html

3.2.1 Physical Access

HSPD-12 compliant credentials must be issued when contractor personnel have more than180 days of unsupervised physical access to a Federally controlled facility during the life of the contract. Contractor personnel that have only intermittent access, of 180 days or less, to federally controlled facilities are not required to undergo the PIV credential process. Contractor personnel with intermittent access include delivery service, vending machine service, and other transient service personnel. If a building is shared with non-government tenants, only access to the Federal area is controlled.

When the initial contract award is 180 days or less, but the contract allows for optional periods of performance that will extend past 180 days, HSPD-12 compliant credentials may be issued.

a. Escorting – A DOC federal employee must sponsor any non-DOC personnel, to allow them escorted access to DOC facilities. However, the sponsoring federal employee may then designate a contractor to provide the physical escorting duties if the contractor has a current PIV, Common Access Card (CAC), or a locally designated permanent badge, and is knowledgeable of the building escort procedures. It is the federal employee's responsibility to ensure the contractor obtains and understands the local escorting procedures. This escort authorization does not extend to the contractor's ability to escort foreign national visitors.

b. See Chapter 30, Facility Protection, of the *Department of Commerce Manual of Security Policies and Procedures* for escort requirements and responsibilities.

3.2.2 Logical Access

If a contractor meets the background investigation requirements for issuance of a CAC or PIV card, that card shall be used as the normal mode of authentication for privileged, unprivileged, and remote Commerce network access on PIV-enabled systems. The COR must document in the Statement of Work the maximum level of access required for the contractor to perform their duties, such as full access for system administration, read/write only access for basic user functions, etc. (see Section II, Chapter 10 of the *Department of Commerce Manual of Security Policies and Procedures* for position designation).

3.2.3 Electronic Infrastructure

Procurements for hardware, software, or services that involve the purchase of hardware or software associated with physical access to DOC facilities or logical access to DOC IT hardware or software (i.e., computer components, servers, local area network components, and other related hardware and software) must be reviewed for compliance with HSPD-12 and FIPS PUB 201. CORs shall coordinate with designated representatives of the Office of Security (OSY) for compliance with physical access requirements and the Office of the Chief Information Officer (OCIO) for compliance with logical access requirements.

3.2.4 End of Service

The COR is responsible for ensuring that government contractors account for all forms of Government-provided identification issued to contractor employees under a contract, i.e., the PIV cards or other similar badges; and shall ensure that contractors return such identification to the issuing agency as soon as any of the following occurs:

a. When no longer needed for contract performance
b. Upon completion of a contractor employee's employment
c. Upon contract completion or termination

In cases involving logical access, the COR should promptly notify, no later than five (5) business days from their departure, the Office of the Chief Information Officer and Office of Security to discontinue service when any of the above situations occurs.

The contracting officer may delay final payment under a contract if the contractor fails to comply with these requirements.

3.3 Service Contracts (non-National Security)

Contractor employees requiring routine access to DOC facilities in order to perform work on 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 for the background check can be obtained from the COR or the Office of Security. Upon receipt of the required forms from the contractor, the COR will forward the forms to the Servicing Security Officer. The Servicing Security Officer will process the forms and advise the COR whether work can commence prior to the completion of the fitness determination based on the type of work and risk to the facility (i.e. adequate controls and restrictions are in place). The COR shall notify the Contracting Officer of the results. The

Contracting Officer (CO) shall notify the Contractor in writing of the approved contract start date, favorable findings of the fitness determination, and the individual's eligibility to be given access to a DOC facility or DOC IT system.

3.3.1 High Risk – Services Contracts

a. Investigative Requirements – All contractor (and subcontractor) personnel proposed to be employed under a "high risk" contract shall undergo a Background Investigation (BI) or the newly approved Federal Investigative Standards[1] for Tier Investigations, which should be updated every five (5) years.

b. Processing Requirements – The contractor must complete and submit the following forms to the COR:

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

   ii. Form FD-258 or SF-87, Fingerprint Card with OPM designation in the Originating Agency Identification (ORI) Block; and

   iii. Credit Release Authorization.

The COR will review these forms for completeness. The Office of Security will notify the COR when the security processing is complete. The COR will provide the results to the CO. The CO shall notify the Contractor in writing of the approved contract start date, favorable findings of the fitness determination, and the individual's eligibility to be given access to a DOC facility or DOC IT system.

3.3.2 Moderate Risk –Service Contracts

a. Investigative Requirements – All contractor (and subcontractor) personnel proposed to be employed under a moderate risk contract shall undergo a Minimum Background Investigation (MBI), or the newly approved Tier 2 investigation, which should be updated every five (5) years. IT-related "moderate risk" positions require the pre-employment check for sensitive and high risk positions. (See Section II, Chapter 11 of the *Department of Commerce Manual of Security Policies and Procedures*).

b. Security Processing Requirement – The contractor must complete and submit the following forms to the COR:

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

   ii. Form FD-258 or SF-87, Fingerprint Card with OPM's designation in the ORI Block; and

   iii. Credit Release Authorization.

The COR will review these forms for completeness. The Office of Security will notify the COR when the security processing is complete. The COR will provide the results to the CO. The CO

[1]Note: Federal Investigations Notice 15-03

shall notify the Contractor in writing of the approved contract start date, favorable findings of the fitness determination, and the individual's eligibility to be given access to a DOC facility or DOC IT system.

3.3.3 Low Risk –Service Contracts for more than 180 days

a. Investigative Requirements – Each person employed under a Low Risk contract shall undergo security processing by the Department's Office of Security as indicated below. Contractors requiring access to a DOC facility for more than 180 days are required to have a National Agency Check with Written Inquiries (NACI), or the newly approved Tier 1 investigation. There is no future periodic investigation requirement at this time.

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

   i. Standard Form 85 (SF-85), Questionnaire for Non-Sensitive Positions;

   ii. Form FD-258 or SF-87, Fingerprint Card;

   iii. Credit Release Authorization

c. All information will be provided to the Servicing Security Officer within 3 business days from start of work, which will send the investigative packet to OPM.

3.3.4 Low Risk Service Contracts for 180 days or less

a. Investigative Requirement for contractors requiring access to a DOC facility for 180 days or less shall have a Special Agreement Check (SAC).

b. Security Processing Requirement – The contractor must complete and submit the following forms to the COR:

   i. Office of Federal Investigations (OFI) Form 86C (OFI-86C), as determined by Chapter 11of the *Department of Commerce Manual of Security Policies and Procedures*.

   ii. FD-258 or SF-87, Fingerprint Card

   iii. Credit Release Authorization

The scope of the SAC will include checks of the Security 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 the minimum of a NACI, or the newly approved Tier 1 investigation conducted to continue working on the job site. Proper designation of the contract/position must be

accomplished in accordance with Section 2 of this manual. The COR shall contact the Servicing Security Office if the duration of the contract will be extended beyond a 180-day period.

3.4 Classified Contracts (National Security)

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 program office representative 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 Security Service (DSS) prior to the release of any National Security information to a Contractor. See Chapter 37, Industrial Security, of the *Department of Commerce Manual of Security Policies and Procedures* for a description of this process.

3.4.2 Investigation Requirements

National Security contracts require the Contractor 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 (5) 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 DSS through the NISPOM process. Guidelines for initiating the investigations are provided in Chapter 37 of the *Department of Commerce Manual of Security Policies and Procedures*. On a case-by-case basis, the Office of Security may grant individual contractors a security clearance for the performance of short-term National Security work. Information on processing this request is contained in Chapter 12, *Department of Commerce Manual of Security Policies and Procedures,* Access to National Security Information.

No National Security materials or documents shall be removed from a DOC facility, without the contractual consent outlined and approved in Form DD-254, Contract Security Classification Specification. 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 employ cleared or clearable U.S. Citizens for positions that may require access to National Security information. In rare circumstances, if cleared or clearable U.S. Citizens are not readily available and a valid rationale for urgent and compelling reasons exists for highly specialized skills or expertise to support a specific U. S. Government contract, a Limited Access Authorization (LAA) may be issued to an Immigrant Alien or a Foreign National. Concurrence of the Director for Security (for highly specialized skills or expertise), and the Department of Defense (in furtherance of U.S. Government obligations pursuant to U.S. law, treaty, or international agreements) is required before issuance of the LAA through the NISPOM process. 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 Chapter 11, Investigative Processing, of the *Department of Commerce Manual of Security Policies and Procedures*.

Permanent Residents 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 *Department of Commerce 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 program office representative (typically the COR) and the Servicing Security Officer work with the Contracting Officer to tailor the provisions to the particular situation. The rationale for the designation shall be documented and placed in the official contract file.

The Contracting Officer shall insert the applicable Federal Acquisition Regulation (FAR) and Commerce Acquisition Regulation (CAR) clause(s) in solicitations and contracts for services.

5.2 Requesting Background Investigations

Once an award is made, the 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 by the Office of Security. 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 *Department of Commerce 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 *Department of Commerce Manual of Security Policies and Procedures,* Chapter 11, and enter the adjudicative decisions in the OPM Personnel Investigations Processing System (PIPS). The Office of Security will provide the results (both favorable and unfavorable findings) in writing to the COR.

The COR shall maintain the contract file pertaining to the fitness determination of their contractor employees. Background information is considered PII and shall not be released. Records should be destroyed as required by the applicable records retention schedule.

5.3.1 Favorable Findings

The COR shall notify the Contracting Officer of the results. The CO shall notify the Contractor in writing of the favorable findings of the fitness determination, and the designation.

5.3.2 Unfavorable Findings

For unfavorable or questionable findings, the COR, in coordination with the Contracting Officer and Servicing 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 contract employee does not meet the fitness 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 fitness determination package. A copy of the notification of the results of the background investigation shall be maintained in the contract file. Additionally, a copy of the notification of results and specific information concerning the subject shall be retained in the Servicing Security Office'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 Officer (CO) – Person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. Includes certain authorized representatives of the contracting officer acting within the limits of their authority as delegated by the contracting officer.

Contracting Officer Representative (COR) – An individual, including a contracting officer's technical representative (COTR), designated and authorized in writing by the contracting officer to perform specific technical or administrative functions.

Federally Controlled Facility – Any Federally owned or leased space, whether single or multi-tenant occupancy, all or any portion of which is under the jurisdiction, custody or control of Department of Commerce.

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.

National Security Information – Executive Order 13526 prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism.

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