Revised – September 2006

COMMERCE ACQUISITION MANUAL
1337.70

DEPARTMENT OF COMMERCE
PERSONNEL SECURITY PROCESSING REQUIRMENTF FOR DEPARTMENT OF COMMERCE SERVICE CONTRACTS

COMMERCE ACQUISITION MANUAL
1337.70

		Page
Section 1	Overview	1
1.1	Purpose	1
1.2	Applicability	1
1.3	Background	1
1.4	Definitions	2
Section 2	Risk Designations and Sensitivity Levels	3
2.1	Non-IT Service Contracts (non-national security)	4
2.2	IT Service Contracts (non-national security)	4
2.3	National Security Contracts	5
Section 3	Background Investigations and Security Processing Requirements	6
3.1	Non-IT Service Contracts (non-national security)	7
3.2	IT Service Contracts (non-national security)	9
3.3	National Security Contracts	10
Section 4	Foreign Nationals (Non-U.S. Citizens)	12
Section 5	Contract Requirements and Procedures	12
5.1	Solicitation/Contract Language	12
5.2	Requesting Background Investigations	13
5.3	Notification of Results	13

ATTACHMENTS

I	Contract Language for Use by Contracting Officers for High or Moderate Risk Contracts	I-1
II	Contract Language for Use by Contracting Officers for Low Risk Contracts	II-1
III	Contract Language for Use by Contracting Officer for National Security Contracts	III-1
IV	Contract Language for Foreign National Visitor and Guest Access to Departmental Resources	IV-1

Personnel Security Processing Requirements for Department of Commerce Service Contracts

Section 1 – Overview

1.1 Purpose

This chapter establishes procedures for adhering to personnel security processing requirements for contractors performing services on or within a Department of Commerce (DOC) facility or through an information technology (IT) system, as required by the Department of Commerce *Security Manual* and Department of Commerce *Security Program Policy and Minimum Implementation Standards*.

1.2 Applicability

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

- Services,
- Involving access to sensitive non-National Security or National Security information, and
- Performed on or within government facilities or through a Department of Commerce network or system.

All Department of Commerce service contracts that meet the criteria above 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 below. The procedures contained herein implement the requirements of the Department of Commerce *Security Manual* for requesting and processing personnel security background investigations.

1.3 Background

Based on Federal laws, regulations, directives, and policies, it is an inherent Government function for a Federal Government 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 is set forth in the Department of Commerce *Security Manual* and

Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*.

1.4 Definitions

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

Contracting Officer Representatives (COR). Individuals with specific authorities delegated from the Contracting Officer to oversee performance and assist with administration of contracts including; monitor and perform specific, enumerated contract management duties related to contract closeout and technical oversight during the performance period of a contract ensuring the contractor's performance meets the standards set forth in the contract, the technical requirements under the contract are met by the delivery date or within the period of performance, and at the price or within the estimated cost stipulated in the contract. A COR may be designated as a Level 1, 2 or 3 Contracting Officer Technical Representative (COTR) or as a Point of Contact/Order Contact (P/OC). All designations are considered Contracting Officer Representatives (CORs).

Foreign National (FNs). Defined as any non-US Citizens or 'Permanent Resident' (defined by U.S. Citizenship and Immigrations Services as "[a]ny person not a citizen of the United States who is residing in the U.S. under legally recognized and lawfully recorded permanent residence as an immigrant." Also know as "Permanent Resident Alien", "Lawful Permanent Resident," "Resident Alien Permit Holder," or "Green Card Holder.") Permanent Resident must provide proof of permanent residency status 30 working days prior to their visit. FNs claiming refugee status or asylum will continue to be governed by the policies outlined in Chapter 16, Foreign National Visitor Access to Departmental Facilities and Activities of the Department of Commerce *Security Manual*, until such time as their cases have been properly adjudicated under the Immigration and Naturalization Act (8 U.S.C. 1157 and 1158 respectively).

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. Guests are subject to a security check at the discretion of the Director for Security.

Information Technology (IT). The term information technology means 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 E.O. 12958).

Operating Unit, Division/Bureau 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 (OSY) that provides security services, support, and guidance to DOC organizations. A servicing security office may provide services and support to a single bureau or may provide services and support to all DOC organizations in a given geographical area.

Section 2 – Risk Designations and Sensitivity Levels

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 work hours; and the extent that 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 procurement COR), in conjunction with operating unit management, cognizant security office, cognizant IT Security Officer, and the procurement office representative. The 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 paragraph 1104 of the *DOC Security Manual).*

2.1 Non-IT Service Contracts (non-National Security). The following risk designations should be used for Non-IT Services Contracts.

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

1. 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;
2. Work involving functions or operations of the Department that are critical to the accomplishment of the mission of the Department;
3. Work involving investigative, compliance, or senior-level auditing duties;
4. Work involving fiduciary, public contact, or other duties involving the highest degree of public trust;
5. Any other work designated High Risk by the head of operating unit or departmental office.

B. Moderate Risk - A contract will be designated Moderate Risk if it meets the following criteria:

1. 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;
2. 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;
3. Work requiring access to sensitive information (information protected under the Privacy Act or Title 13 of the U.S. Code); or
4. Work involving foreign travel less than 90 days duration.

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

2.2 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 the Department of Commerce *IT Security Program Policy and Minimum Implementation Standards*, Chapter 7, Section 7.4.

A. **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 Office staff).

B. **Moderate Risk**: "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 in it (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

C. **IT-Low**: Users with access to a DOC local area network, e-mail, basic office applications (such as Microsoft Office or Corel Office suites), 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 risk designation depends on the security categorization of the system(s) involved.

2.3 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 43, Industrial Security, of the *DOC Security Manual.*

All employee positions in the Department of Commerce require a risk designation. In addition, positions that require 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.

A. **Special Sensitive** – include any positions 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 E.O. 10450 and E.O. 12968 (such as DCID 6/4 that sets investigative requirements and standards for access to Sensitive Compartmented Information (SCI) and other intelligence-related Special Sensitive information.

B. **Critical Sensitive** – are positions that have potential for exceptionally grave damage to the national security. These positions may include access to, and including, 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 duty on personnel security boards; or other positions related to national security, regardless of duties, that require the same degree of trust.

C. **Non-critical Sensitive** – are 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.

Section 3 – Background Investigations and Security Processing Requirements

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 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.

Copies of the appropriate forms can be obtained from the COR or the Office of Security. Upon receipt of the required forms, the COR 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 COR will notify the Contractor of an approved contract start date as well as favorable or unfavorable finding of the suitability determinations.

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

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

A. High Risk – Non-IT Services Contracts.

Investigative Requirments. 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.

Processing Requirements. The contractor must complete and submit the following forms to the Contracting Officer Representative (COR):

- Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
- FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
- Credit Release Authorization.

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 Department of Commerce facility or Department of Commerce IT system.

B. Moderate Risk – Non-IT Service Contracts

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.

Security Processing Requirement. The contractor must complete and submit the following forms to the Contracting Officer Representative (COR):

- Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
- FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
- Credit Release Authorization.

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 Department of Commerce facility or Department of Commerce 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 CIS (formerly INS) agency check. It is the option of the Office of Security to repeat the security processing on any contract employee at its discretion.

C. Low Risk – Non-IT Service Contracts

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

1. Contracts employees requiring access to Department of Commerce 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 SF-85, Questionnaire for Non-Sensitive Positions, Form FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer within three working days from start of work, who will send the investigative packet to the Office of Personnel Management.

2. Contracts employees requiring access to a Department of Commerce facility for less than 180 days shall have a Special Agency Check (SAC), as determined by Department of Commerce *Security Manual*, Chapter 11. The Contracting Officer's Representative (COR) will forward a completed Form OFI-86C, FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer, who will send the investigative packet to the Office of Personnel Management 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 (Customs and Immigration Service) check on the SAC, Form OF-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 Special Agreement Check 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.

3.2 IT Service Contracts (non-national security)

Individuals employed in High Risk positions, or Moderate Risk positions in the IT occupations, 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.

A. High Risk – IT Contracts

Investigative Requirement. All contractor (and subcontractor) personnel proposed to be employed under a IT High Risk contract shall undergo a Background Investigation (BI).

Security Processing Requirement. The contractor must complete and submit the following forms to the Contracting Officer Representative (COR):

- Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
- FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
- Credit Release Authorization.

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 Department of Commerce facility or Department of Commerce IT system.

B. Moderate Risk - IT Contracts

Investigative Requirement. All contractor (and subcontractor) personnel proposed to be employed under a IT Moderate Risk contract shall undergo a Background Investigation (BI).

Security Processing Requirement. The contractor must complete and submit the following forms to the Contracting Officer Representative (COR):

- Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
- FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
- Credit Release Authorization.

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. c. 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 Department of Commerce facility or Department of Commerce IT system.

C. Low Risk – IT Contracts

Investigative Requirements. Contract employees employed in all Low Risk IT service contracts will require a National Agency Check and Inquiries (NACI) to be processed

Security Processing Requirements. The COR will forward a completed Form SF-85, Form FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer within three working days from start of work, who will send the investigative packet to the Office of Personnel Management. 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 NAC.

3.3 National Security Contracts

Risk Assessment

Before requesting background investigations for personnel performing work on a 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 National Security Information. The Contracting Officer (CO) and Contracting Officer's Representative (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 CO must obtain verification 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 43, Industrial Security, of the Department of Commerce *Security Manual* for a description of this process.

Investigation Requirements
National Security contracts require employed contractors to gain access to national security information in the performance of their work. Regardless of the contractor, consultant, or expert's location, appropriate security access and fulfillment of cleared facility requirements as determined by the National Industrial Security Program Operation Manual (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. No national security material or documents shall be removed from a Department of Commerce facility. The circumstances of the work performance must allow the Department of Commerce to retain control over the information and keep the number of contract personnel with access to a minimum.

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 (10) years.

Security Processing Requirements
Contract employees of National Security contracts must complete and submit the following forms to the Contracting Officer Representative (COR):

- Form SF-86, Questionnaire for National Security Positions, marked "CON" in Block 1, Position Title, to distinguish it as a contractor case;
- Form FD-258, Fingerprint Chart, with OPM's designation in the ORI Block; and
- Credit Release Authorization Form.

The COR must send the contract employee's existing security clearance information, if applicable, or appropriate investigative request package to the servicing Security Officer who will review and forward it to the Office of Security Headquarters. The COR must review the request package for completeness, ensuring that the subject of each package is identified as a contract employee, the name of the contractor is identified, and that each package clearly indicates the contract sensitivity designation. The Office of Security must confirm that contract employees have the appropriate security clearance before starting any national security work. The Servicing Security Officer must forward the request for investigation to the Defense Investigative Service Coordinating Office (DISCO), maintain records of contractor/consultant personnel in their units subject to the NISP, and ensure that all contractor personnel have been briefed on the appropriate procedures for handling and safeguarding national security information.

Additional Considerations for National Security Contracts
Only U.S. citizens are eligible to obtain a security clearance. Once the sensitivity level of the contract has been determined, the COR will obtain completed personnel security

investigation forms from individuals proposed to perform work on the contract and submit the forms to the Office of Security for processing. Security clearances for personnel performing work on a national security contract must be granted by DISCO through the NISPOM (National Industrial Security Program Operating Manual) process. Appendix C, Minimum Requirements for Personnel Investigations, of the Department of Commerce *Security Manual* provides the requirements for investigative processing of contract employees requiring access to national security information. Guidelines for initiating the investigations are provided in Appendix D, Processing Personnel Security and Suitability Investigations, paragraph D.3, Processing Investigations. 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 Appendix E of the Department of Commerce *Security Manual*, Obtaining Access to Classified Information.

Section 4 - Foreign Nationals (Non- U.S. Citizens)

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 skill 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. In addition, the Limited Access Authorization may only be issued through the NISPOM clearance. 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. Additional criteria for Non- U.S. Citizens are described in the Department of Commerce *Security Manual,* Chapter 16.

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

Section 5 -- Contract Requirements and Procedures

5.1 Solicitation/Contract Language

All solicitations/contracts that meet the criteria in Section 1.2 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/Contract Specialist to tailor the provision to the particular situation. The rationale for the designed risk level shall be documented and placed in the official contract file.

A. Attachment I, CAR clause 1352.237-71 contains contract language for Non-IT and IT service contracts with High and Moderate Risk designations.

B. Attachment II, CAR clause 1352.237-72 contains contract language for Non-IT and IT service contracts with Low Risk designation.

C. Attachment III, CAR clause 1352.237-73 contains contract language for contracts designated as National security.

D. Attachment IV, CAR clause 1352.237-74 contains contract language for foreign national visitor and guest access to Departmental resources.

5.2 Requesting Background Investigations

Once an award is made, the COR as a Personal Identity Verification (PIV) sponsor is responsible for following procedures for the PIV credential process as specified at the Department of Commerce Office of Security website, http://www.osec.doc.gov/osy/HSPD12/HSPD-12Information.htm . Work may not commence until the contract employees have been granted eligibility for access to a Department of Commerce facility or IT system. There are differences in the timing of 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 CAR clause 1352.237-73, based on criteria found in Appendix E, Paragraph D.1, D.2 and E.1 of the Department of Commerce *Security Manual*.

5.3 Notification of Results

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

A. 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.

B. 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 opinions 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 Contracting Officer 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. Finally, 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.

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 chapter 13, section 13.8 of the Department of Commerce *IT Security Program Policy* for more information on approved methods that may be applied to both paper and electronic media.

Attachment I

Contract Language for Use by Contracting Officers for High or Moderate Risk Contracts

The Contracting Officer shall insert the following clause in all service contracts designated as High or Moderate Risk that will be performed within a Department of Commerce facility or through a Department of Commerce IT system:

1352.237-71 ***Security Processing Requirements for Contractor/Subcontractor Personnel Working on a Department of Commerce Site or IT System (High or Moderate Risk Contracts)***

A. Investigative Requirements for High and Moderate Risk Contracts

All contractor (and subcontractor) personnel proposed to be employed under a High or Moderate Risk contract shall undergo security processing by the Department's Office of Security before being eligible to work on the premises of any Department of Commerce facility, or through a Department of Commerce IT system. All Department of Commerce security processing pertinent to this contract will be conducted at no cost to the contractor. The level of contract risk will determine the type and scope of such processing as noted below.

1. Non-IT Service Contracts

   a. High Risk – Background Investigation (BI)
   b. Moderate Risk – Moderate Background Investigation (MBI)

2. IT Service Contracts

   a. High Risk IT – Background Investigation (BI)
   b. Moderate Risk IT – Background Investigation (BI)

3. In addition to the investigations noted above, non-U.S. citizens must have a pre-appointment check that includes a Customs and Immigration Service (CIS – formerly Immigration and Naturalization Service) agency check.

B. Additional Requirements for Foreign Nationals (Non-U.S. Citizens)

To be employed under this contract within the United States, non-U.S. citizens must have:

- Official legal status in the United States
- Continuously resided in the United States for the last two years; and
- Advance approval from the servicing Security Officer of the contracting operating unit in consultation with the Office of Security (OSY) headquarters. (OSY routinely consults with appropriate agencies regarding the use of non-U.S. citizens on contracts and can provide up-to-date information concerning this matter.)

C. Security Processing Requirement

1. Processing requirements for High and Moderate Risk Contracts are as follows:

   a. The contractor must complete and submit the following forms to the Contracting Officer Representative (COR):

      - Standard Form 85P (SF-85P), Questionnaire for Public Trust Positions;
      - FD-258, Fingerprint Chart with OPM's designation in the ORI Block; and
      - Credit Release Authorization.

   b. 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.

   c. 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 Department of Commerce facility or Department of Commerce IT system.

2. 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 an Immigration and Customs Enforcement (formerly INS) agency check. It is the option of the Office of Security to repeat the security processing on any contract employee at its discretion.

D. Notification of Disqualifying Information

If the Office of Security receives disqualifying information on a contract employee, the COR will be notified. The COR, in coordination with the contracting officer, will

immediately remove the contract employee from duty requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following:

- Conviction of a felony of a crime of violence or of a misdemeanor involving moral turpitude.
- Falsification of information entered on security screening forms or of other documents submitted to the Department.
- Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct directly related to the contract.
- Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

NOTE: Failure to comply with the requirements may result in termination of the contract or removal of some contract employees from Department of Commerce facilities or access to IT systems.

E. Access to National security Information

Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

F. The Contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of Clause)

Attachment II

Contract Language for Use by Contracting Officers for Low Risk Contracts

The Contracting Officer shall insert the following clause in all service contracts designated as Low risk that will be performed on or within a Department of Commerce facility or through Department of Commerce IT system:

1352.237-72 ***Security Processing Requirements for Contractor/Subcontractor Personnel Working on a Department of Commerce Site (Low Risk Contracts)***

A. Investigative Requirements for Low Risk Contracts

Each person employed under this Low Risk contract shall undergo security processing by the Department's Office of Security as indicated below before being eligible to work on the premises of any Department of Commerce owned, leased, or controlled facility in the United States or overseas or obtain access to a DOC IT system. All Department of Commerce security processing pertinent to this contract will be conducted at no cost to the contractor.

1. Non-IT Service Contracts

   a. Contracts more than 180 days – National Agency Check and Inquiries (NACI)
   b. Contracts less than 180 days – Special Agency Check (SAC)

2. IT Service Contracts

   a. Contracts more than 180 days – National Agency Check and Inquiries (NACI)
   b. Contracts less than 180 days – National Agency Check and Inquiries (NACI)

3. In addition to the investigations noted above, non-U.S. citizens must have a background check that includes an Immigration and Customs Enforcement (ICE – formerly Immigration and Naturalization Service) agency check.

B. Additional Requirements for Foreign Nationals (Non-U.S. Citizens)

Non-U.S. citizens (lawful permanent residents) to be employed under this contract within the United States must have:

- Official legal status in the United States;
- Continuously resided in the United States for the last two years; and
- Advance approval from the servicing Security Officer in consultation with the Office of Security headquarters.

C. Security Processing Requirements for Low Risk Non-IT Service Contracts

Processing requirements for Low Risk non-IT Service Contracts are as follows.

1. Contract employees employed in Low Risk non-IT service contracts for more than 180 days will require a National Agency Check and Inquiries (NACI) to be processed. The COR will forward a completed Standard Form SF-85, Questionnaire for Non-Sensitive Positions, Form FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer within three working days from start of work, who will send the investigative packet to the Office of Personnel Management.

2. Contract employees employed in Low Risk non-IT service contracts for less than 180 days require a Special Agreement Check (SAC), Form OFI-86C, to be processed. The Contracting Officer's Representative (COR) will forward a completed Form OFI-86C, FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer, who will send the investigative packet to the Office of Personnel Management for processing.

3. Any contract employee with a favorable Special Agreement Check who remains on the contract over 180 days will be required to have a NACI conducted to continue working on the job site.

4. For Low Risk non-IT service contracts, 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).

5. In addition, for those individuals who are not U.S. citizens (lawful permanent residents), the COR must request a CIS (Customs and Immigration Service) check on the SAC, Form OF-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.

6. Copies of the appropriate forms can be obtained from the COR or the Office of Security. Upon receipt of the required forms, the COR 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 COR will notify the Contractor of an approved contract start date as well as favorable or unfavorable finding of the suitability determinations.

D. Security Processing Requirements for Low Risk IT Service Contracts

Processing requirements for Low Risk IT Service Contracts are as follows.

1. Contract employees employed in all Low Risk IT service contracts will require a National Agency Check and Inquiries (NACI) to be processed. The COR will forward a completed Form SF-85, Form FD-258, Fingerprint Chart, and Credit Release Authorization to the servicing Security Officer within three working days from start of work, who will send the investigative packet to the Office of Personnel Management.

2. For Low Risk IT service contracts, individuals who are not U.S. citizens (lawful permanent residents) must undergo a NACI that includes an agency check conducted by the Customs and Immigration Service (CIS). The COR must request the CIS check as a part of the NAC.

E. Notification of Disqualifying Information

If the Office of Security receives disqualifying information on a contract employee, the COR will be notified. The COR, in coordination with the Contracting Officer, will immediately remove the employee from duty requiring access to Departmental facilities or IT systems. Contract employees may be barred from working on the premises of a facility for any of the following reasons:

- Conviction of a felony of a crime of violence or of a misdemeanor involving moral turpitude.
- Falsification of information entered on security screening forms or of other documents submitted to the Department.
- Improper conduct once performing on the contract, including criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct or other conduct prejudicial to the Government regardless of whether the conduct directly related to the contract.
- Any behavior judged to pose a potential threat to Departmental information systems, personnel, property, or other assets.

NOTE: Failure to comply with the requirements may result in termination of the

contract or removal of some contract employees from Department of Commerce facilities.

F. Access to National security Information

Compliance with these requirements shall not be construed as providing a contract employee clearance to have access to national security information.

G. The Contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of Clause)

Attachment III

Contract Language for Use by Contracting Officers for National Security Contracts

The Contracting Officer shall insert the following clause in all service contracts designated as national security that will be performed on or within a Department of Commerce facility or through a Department of Commerce IT system:

1352.237-73 Security Processing for Contractor/subcontractor Personnel Working on a Department Of Commerce Site (National security Contracts)

A. Security Investigative Requirements for National security Contracts.

National security contracts require employed contractors to gain access to national security information in the performance of their work. Regardless of the contractor, consultant, or expert's location, appropriate security access and fulfillment of cleared facility requirements as determined by the National Industrial Security Program Operation Manual (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. No national security material or documents shall be removed from a Department of Commerce facility. The circumstances of the work performance must allow the Department of Commerce to retain control over the information and keep the number of contract personnel with access to a minimum.

1. Special Sensitive or Critical Sensitive.

2. Non-Critical Sensitive.

3. 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 (10) years.

B. Security Procedures

Position sensitivity/risk assessments must be conducted on all functions that are performed by the contract. Risk assessments are determined in the same manner as those functions performed by employees. The Contracting Officer (CO) and Contracting Officer Representative (COR) should determine the level of sensitivity or risk with the assistance of the servicing Security Officer.

1. Contract employees of national security contracts must have a completed investigation and be granted an appropriate level security clearance by the Office of Security headquarters, before start of work.

2. The COR must send the contract employee's existing security clearance information, if applicable, or appropriate investigative request package to the servicing Security Officer who will review and forward it to the Office of Security Headquarters.

3. The Office of Security must confirm that contract employees have the appropriate security clearance before starting any national security work.

C. Security Forms Required

For Critical-Sensitive positions with Top Secret access, Critical-Sensitive positions with Secret access, and Non-Critical Sensitive positions with Secret or Confidential access, the following forms are required:

1. Form SF-86, Questionnaire for National Security Positions, marked "CON" in Block 1, Position Title, to distinguish it as a contractor case;

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

3. Credit Release Authorization Form.

D. Contracting Officer Representative (COR) Responsibilities

1. Coordinate submission of proper investigative request package with the servicing Security Officer, the Contracting Officer (CO), and the contractor.

2. Review the request package for completeness, ensuring that the subject of each package is identified as a contract employee, the name of the contractor is identified, and that each package clearly indicates the contract sensitivity designation.

3. Send the request package to the servicing Security Officer for investigative processing.

E. Servicing Security Officer Responsibilities

1. Review the package for completeness.

2. Ensure that the forms are complete and contain all the pertinent information necessary to request the background investigation.

3. Forward the request for investigation to the Defense Investigative Service

Coordinating Office (DISCO).

4. Maintain records of contractor/consultant personnel in their units subject to the NISP.

5. Ensure that all contractor personnel have been briefed on the appropriate procedures for handling and safeguarding national security information.

F. The Contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of Clause)

Attachment IV

Contract Language for Foreign National Visitor and Guest Access to Departmental Resources

The Contracting Officer shall insert a clause the same as the following in all service contracts where foreign national access to any Department of Commerce facility or through a Department of Commerce IT system is required. The following language may only be modified by adding more restrictive agency or bureau specific guidance.

1352.237-74 Foreign National Visitor and Guest Access to Departmental Resources

The Contractor shall comply with the provisions of Department of Commerce Administrative Order 207-12, Foreign National Visitor and Guest Access Program http://dms.osec.doc.gov/cgi-bin/doit.cgi?204:112:b5642b6417d6e6ab51e6b745ffabf4fc40abebfadd74c8df0bf7998dc3e45fea:256; Bureau of Industry and Security Export Administrative Regulations Part 734, http://www.gpo.gov/bis/ear/pdf/734.pdf, and [insert Bureau specific procedures]. The contractor shall provide the government with notices of foreign nationals requiring access to any Department of Commerce facility or through a Department of Commerce IT system

The Contractor shall identify each foreign national who requires access to any Departmental resources, and shall provide all requested information in writing to the Contracting Officer Representative.

The Contractor shall include the substance of this clause, including this paragraph, in all subcontracts.

(End of Clause)