Revised – June 2024

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, contractor personnel granted access to a federally controlled facility, permanent access to a federal information system, or access to Classified National Security Information (CNSI) shall be subject to security screening requirements similar to those imposed upon federal personnel. Personnel security investigative requirements for access to a federally controlled facility, access to a federal information system, or access to CNSI are set forth in the Department of Commerce's *Manual of Security Policies and Procedures*, December 2012, and the Department of Commerce's *Enterprise Cybersecurity Policy, September 2022*.

1.2. Purpose

The purpose of this Commerce Acquisition Manual (CAM) chapter is to identify the procedures required for adhering to Department of Commerce (DOC or Department) security processing requirements for contractor personnel.

1.3. Applicability

The requirements of this chapter are applicable to solicitations and contracts that meet the following criteria:

a. Services involving access to Controlled Unclassified Information (CUI) or CNSI; or

b. Services performed on or within Departmental or other federal facilities[1] or through a Departmental information technology (IT) network or system.

END OF SECTION 1

[1] Excluding non-federal short-term visitors on official business.

SECTION 2 - DESIGNATING CONTRACTS

2.1. Designation Factors

A contract designation is required to determine the appropriate security processing requirements for contractor personnel performing services in accordance with Section 1.3. This designation is determined by evaluating the following:

a. The risk or sensitivity of the work being planned and the facility in which the work is to be performed;

b. The security impact level of the IT system to which government personnel and non-government personnel have access;

c. The level of access privileges to an IT system;

d. Whether the contracted activities are to be performed during or outside of normal business hours; and

e. The extent that a government escort will be both necessary and available to the contractor personnel present in the facility or while IT access is required.

2.2. Risk Levels

The program office representative, typically the Contracting Officer Representative,[2] shall review the work to be performed and consult with the program office management, Information Technology Security Officer, Security Office, and/or procurement office to determine the appropriate risk and sensitivity level designation. 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 (PDT). For more information regarding these designations, see the *Manual of Security Policies and Procedures*[3]. The following designations may be assigned:

a. Low Risk Contract: A contract shall be designated as "low risk" if it does not meet any of the criteria for "high risk" or "moderate risk" due to lower risk factors.

b. Moderate Risk Contract: A contract shall be designated "moderate risk" if it meets the criteria as determined by the OPM PDT.

c. High Risk Contract: A contract shall be designated "high risk" if it meets the criteria as determined by the OPM PDT.

d. National Security Contract: A National Security Contract is often referred to as a Classified Contract and meets the following criteria:

[2] For pre-award activities, a Contracting Officer Representative may not have been appointed, therefore this may be another individual as determined by the manager of the respective program.

[3] Links to the PDT, forms, and the Manual of Security Policies and Procedures may be found on the Office of Security's website at https://www.commerce.gov/osy.

i. Contractors require continuous access to CNSI or Sensitive Compartmented Information (SCI); and

ii. Work to be performed on the contract falls within one of the eight categories covered in Executive Order 13526, Section 1.4, "Classification Categories."

END OF SECTION 2

SECTION 3 - CONTRACT REQUIREMENTS AND PROCEDURES

The following subsections identify the requirements for the acquisition workforce in executing contracts required by Section 1.3. The requirements and procedures have been separated by Low, Moderate, High, or the National Security Contract designation and identified by the phase of the acquisition.

3.1 Low, Moderate, or High Risk Contracts

3.1.1 Pre-solicitation

a. The program office representative shall assign the highest risk or sensitivity designation to the entire contract, in accordance with the criteria outlined in Section 2 and the *Manual of Security Policies and Procedures*, and record the designation in the acquisition planning documents and the security requirements section of the requirements document (Statement of Work [SOW], Statement of Objectives [SOO] or Performance Work Statement [PWS]). The rationale for the designated risk level shall be documented and provided to the Contracting Officer for placement in the contract file.

b. For logical access, the program office representative must record in the requirements document 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.

c. 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 Homeland Security Presidential Directive 12 (HSPD-12) and Federal Information Processing Standard Publication 201 (FIPS PUB 201). The program office representative shall coordinate with designated representatives of the Security Office for compliance with physical access requirements and the Office of the Chief Information Officer (OCIO) for compliance with logical access requirements.

d. The program office representative shall notify the Contracting Officer when foreign national access to any DOC facility or DOC IT system is required and ensure compliance with the provisions of Department Administrative Order 207-12, Foreign Access Management Program.

3.1.2 Solicitation

a. The Contracting Officer shall use the designation and other information supplied by the program office representative and documented in the SOW, PWS, or SOO to determine the applicable Federal Acquisition Regulation (FAR) and Commerce Acquisition Regulation (CAR) provision(s) and clause(s). See FAR 4.4 and CAR 1337 for additional information.

b. The Contracting Officer shall ensure the applicable provisions and clauses are included in the solicitation and subsequent contract as well as a security section tailored to the access required in the performance of the contract.

3.1.3 Award

3.1.3.1 Background Investigations

a. Contractor personnel requiring routine access to Department facilities or systems to perform work on Department service contracts that do not require access to CNSI must undergo a background check based on the risk level of the contract. After the award of a contract, the Contracting Officer Representative shall coordinate with their Security Office to submit the required forms. The Security Office will process the forms in accordance with the *Manual of Security Policies and Procedures* and advise the Contracting Officer Representative 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).

b. For favorable pre-appointment and investigative determinations, the Contracting Officer Representative shall notify the Contracting Officer of the results. The Contracting Officer, or Contracting Officer Representative if delegated, shall notify the contractor in writing of the approved contract start date, the approved contract end date, favorable findings of the fitness determination, and the individual's eligibility to be given access to a Department facility or Department IT system at a Department or contractor facility.

c. The notification of the results that a given contractor personnel does not meet the fitness or sensitivity requirements for the contract shall be made in writing by the Security Office directly to the contractor and Contracting Officer Representative. Requests for further information needed to make a fitness determination shall be made in writing by the Security Office 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.

3.1.3.2 HSPD-12 Credentialing

a. PIV/CAC Cards: HSPD-12 compliant credentials, such as Personal Identity Verification (PIV) cards and Common Access Cards (CAC), must be issued to contractor personnel who need regular or routine unescorted access to federal facilities and/or information technology systems for a period of six months or longer during the life of the contract. If the initial contract award is for six months or less but allows for optional periods of performance that will extend past six months, HSPD-12-compliant credentials may still be issued.

   When contractor personnel require intermittent or transient (i.e., not regular or routine) access to federal facilities and/or technology systems, the bureau or Security Office may choose not to issue credentials to the contractor. Examples of intermittent or transient personnel include, but are not limited to, delivery services, vending machine servicing, maintenance, shred services, or other personnel requiring similar access.

b. Alternate Authenticator Credentials: Contractor personnel that have short-term access of six months or less to federally controlled facilities and/or information technology systems are not required to undergo the credentialling process.

After a favorable security determination of a short-term worker, bureaus may issue an alternative authenticator, such as a PIV Interoperable (PIV-I) card, a Facility Access Card (FAC), or similar approved temporary proximity card.

PIV-I cards or alternative authenticators may be appropriate for situations where an agency has determined that a PIV card is not warranted, but the individual requires access. Such situations may include, but are not limited to:

i. Temporary/seasonal employees, visiting scientists and guest researchers, or contractor personnel requiring access for less than six months;

ii. Non-U.S. nationals with insufficient residency in the U.S. to satisfactorily conduct the background investigation; and

iii. Personnel operating outside the contiguous U.S. under special risk security considerations, as outlined in FIPS 201.

3.1.3.3 HSPD-12 Credentialing Procedures

a. A badge sponsor, which is the Contracting Officer Representative and/or other individual as determined by the manager of the respective program, shall be assigned to assist contractor personnel during the initial vetting and credentialing process, and when credentials are renewed or rescinded.

b. For programs within the National Oceanic and Atmospheric Administration (NOAA), the National Institute of Standards and Technology (NIST), and the U.S. Census Bureau (Census) that require a contractor to have a badge, the Contracting Officer Representative should follow the standard operating procedures for sponsorship for the security offices within those bureaus.

c. For programs not within NOAA, NIST, or Census that require a contractor to have a badge, the Contracting Officer Representative should complete a Contractor Sponsorship Form[4] and submit it to HSPD-12@doc.gov.

d. The badge sponsor shall submit the applicable documents to their respective badge issuing office within five business days after the award of a contract.

e. Contractor personnel may only be issued PIV cards after the required background checks have been completed and only on or after the official start date designated by the Contracting Officer Representative.

3.1.4 Post-Award

a. Where credentials are not issued, a DOC federal employee must sponsor individuals to provide them with escorted access to DOC facilities. The sponsoring federal employee may then designate a contractor to provide the physical escorting duties if the contractor has a current PIV, CAC, or a locally designated permanent badge and is knowledgeable of the

[4] The Contractor Sponsorship Form contains Personally Identifiable Information and, as such, shall be protected went sent via email.

building escort procedures. It is the federal employee's responsibility to ensure the contractor understands and adheres to the local escorting procedures. This escort authorization does not extend to the contractor's ability to escort foreign national visitors.

b. If a contractor meets the background investigation requirements for the issuance of a CAC or PIV card, that card shall be used as the normal mode of authentication for privileged, unprivileged, and remote DOC network access on PIV-enabled systems.

c. The Contracting Officer Representative is responsible for ensuring government contractors account for all forms of government-provided identification and keys issued to contractor personnel under a contract (i.e., PIV, CAC, or similar badges) and shall ensure that contractors return such items to the issuing office immediately, when any of the following occurs:

   i. When no longer needed for contract performance.

   ii. Upon the completion of a contractor personnel's employment.

   iii. Transfer of contractor to another contract.

   iv. Upon contract completion or termination.

   In the event the government-provided credential or keys are not collected and returned, the Security Office must be notified immediately.

   The Contracting Officer may delay final payment under a contract if the contractor fails to return these items.

d. In cases involving logical access, the Contracting Officer Representative shall notify the OCIO no later than five business/duty days from contractor departure.

e. The Contracting Officer Representative shall notify the Security Office no later than five business/duty days from contractor departure. **This applies to *all* contractor personnel** leaving Department contracts, transferring between contracts, or changing their clearance access level.

3.2 National Security Contracts

3.2.1 Pre-Solicitation

a. Prior to the release of the solicitation, the Contracting Officer Representative shall coordinate with the Industrial Security Program (ISP), which is part of the Department of Commerce's Office of Security. To coordinate with the ISP, the Contracting Officer Representative will complete the Office of Security (OSY) Industrial Security Intake Form and submit the following documents to OSY_IndustrialSecurity@doc.gov:

   i. Draft DD Form 254, Contract Security Classification Specification (DD-254): The DD-254 conveys security requirements to contractors when contract performance requires access to CNSI. Prime contractors also use the DD-254 to convey security requirements to subcontractors that require access to CNSI to perform on a

subcontract.

ii. Requirements document (PWS, SOW, etc.): The requirements document must outline the classified work to be performed and clearly state how and why the contractor will require continuous access to CNSI, at what level (Confidential, Secret, Top Secret), to what extent (meetings, direct access to classified material, or access to classified systems), and which task(s) are associated with access to CNSI.

b. The ISP will produce a Draft DD-254 for the Contracting Officer Representative to provide to the Contracting Officer.

3.2.2 Solicitation

a. The Contracting Officer shall ensure that the solicitation contains all needed security provisions and clauses based on the contract designation. See FAR 4.4 and Commerce Acquisition Regulation CAR 1337 for additional information.

b. The Contracting Officer will ensure the draft DD-254 has been reviewed and approved by the ISP and is included in/with the solicitation.

3.2.3 Prior to Award

a. The Contracting Officer Representative will perform the following steps:

i. Obtain verification that the contractor's facility is in possession of a valid Facility Clearance Level equal to or greater than the clearance level of the contract.

ii. Submit the following documents to OSY_IndustrialSecurity@doc.gov:
1. Draft DD-254
2. Final requirements document (PWS, SOW, etc.)
3. Draft SF-1449, SF-30, OF-347, or equivalent contract form(s)

b. The ISP will issue an approved DD-254.

c. The Contracting Officer will include the approved DD-254 with the contract award.

3.2.4 Award

3.2.4.1 Documentation

a. The Contracting Officer Representative will submit the following documents to OSY_IndustrialSecurity@doc.gov:

i. Visitor Access Request (VAR) on the contractor's letterhead.[6]

ii. SF-312, Classified Information Nondisclosure Agreement.

[6] VARs contain Personally Identifiable Information and, as such, shall be protected when sent via email.

iii. A CNSI Training Certificate that indicates that training has been completed via the Department of Commerce's CNSI training.

b. If the prime contractor awards a subcontract that requires access to CNSI, the Contracting Officer Representative should ensure a DD-254 is completed by the prime contractor and submit it to the ISP.

3.2.4.2 Credentialing

a. A badge sponsor, which is the Contracting Officer Representative and/or other individual as determined by the manager of the respective program, shall be assigned to assist contractor personnel during the initial vetting and credentialing process and when credentials are renewed or rescinded.

b. For programs within NOAA, NIST, and Census that require a contractor to have a badge, the Contracting Officer Representative should follow the standard operating procedures for sponsorship for the security offices within those bureaus.

c. For programs not within NOAA, NIST, or Census that require a contractor to have a badge, the Contracting Officer Representative should complete a Contractor Sponsorship Form[7] and submit it to HSPD-12@doc.gov.

d. The badge sponsor shall submit the applicable documents to their respective badge issuing office within five business days after the award of a contract.

e. Contractor personnel may only be issued PIV cards after the required background checks have been completed and only on or after the official start date designated by the Contracting Officer Representative.

3.2.5 Post-Award

a. The Contracting Officer Representative should ensure that the DD-254 and language in the requirements document is reviewed every two years with the ISP to ensure the Facility Clearance Level, place of performance, and security requirements are current.

b. The Contracting Officer Representative shall ensure that a VAR is submitted annually to OSY_IndustrialSecurity@doc.gov.

c. The Contracting Officer Representative should ensure that a CNSI Training Certificate is submitted annually to OSY_IndustrialSecurity@doc.gov.

d. Upon contract conclusion, the Contracting Officer Representative should execute a final DD-254 in coordination with the ISP and submit it to the cognizant Defense Counterintelligence Security Agency (DCSA) office.

e. The Contracting Officer Representative shall send notice of separation, within five business/duty days after the separation, to the ISP at OSY_IndustrialSecurity@doc.gov for cleared contractors working on classified contracts. This applies to all contractor personnel

[7] The Contractor Sponsorship Form contains Personally Identifiable Information and, as such, shall be protected went sent via email.

leaving Department contracts, transferring between contracts, or changing clearance access level.

f. The Contracting Officer Representative shall also provide notice of all contractor personnel separating no later than five business/duty days prior to the conclusion/date performed under any contract to the servicing Security Office to deactivate the contractor's record in Security Manager. Additional notice shall be sent to the Special Security Officer (SSO) via DSSO@doc.gov to deactivate Sensitive Compartmented Information (SCI) access, as applicable. These changes will be reflected in Security Manager and USAccess records.

END OF SECTION 3
END OF CAM 1337.70

APPENDICES

APPENDIX A: Definitions

Badge: Identification cards used government-wide to access federally controlled facilities and information systems at the appropriate security level. They can include PIV cards, CACs, and Facility Access Cards (FACs).

Cleared Contractors: Person who has been vetted through the Security Office found to have a current security clearance authorizing access CNSI.

Contracting Officer (CO): Person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings. This includes certain authorized representatives of the Contracting Officer acting within the limits of their authority, as delegated by the CO.

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

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.

Security Office: Office of Security headquarters or Field Servicing Security Office that provides security services, support, and guidance to a single bureau or to all Department organizations in a given geographical area. Security offices shall be managed by the designated Director of Security.

APPENDIX B: Reference Documents

a. DOC *Manual of Security Policies and Procedures* Section III, Classified National Security Information, and Section IV, Chapter 37, Industrial Security (DEC 2012)

b. *National Industrial Security Program Operating Manual*

c. 32 *The Code of Federal Regulations* (CFR) Part 117 (FEB 2022)

d. 32 CFR Part 2004, NISP

e. Department of Defense (DoD) Manual 5220.32 Volume 1 *National Industrial Security Program: Industrial Security Procedures for Government Activities* (DEC 2021)

f. Federal Acquisition Regulation (FAR) Clause 52.204.2, Security Requirements (Mar 2021)

g. FAR Subpart 4.4 – Safeguarding Classified Information Within Industry (JUN 2023)

h. Commerce Acquisition Regulation (CAR) Clause 1352.237-70, Security processing requirements – high or moderate risk contracts

i. National Industrial Security Program, Executive Order (EO) 12829 (FEB 2016)

j. Intelligence Community Directive (ICD) 704.2

k. Security Executive Agent Directive 3 (JUN 2017)

l. Security Executive Agent Directive 6 (JAN 2018)

m. Executive Order 13467