DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 117

[Docket ID: DOD–2020–OS–0045]

RIN 0790–AK85

National Industrial Security Program Operating Manual (NISPOM)

AGENCY: Office of the Under Secretary of Defense for Intelligence & Security, Department of Defense (DoD).

ACTION: Final rule with request for comment.

SUMMARY: The Department of Defense (DoD) is codifying the National Industrial Security Program Operating Manual (NISPOM) in regulation. The NISPOM establishes requirements for the protection of classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders (hereinafter referred to as contractors) to prevent unauthorized disclosure. In addition to adding the NISPOM to the Code of Federal Regulations (CFR), this rule incorporates the requirements of Security Executive Agent Directive (SEAD) 3, ''Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position.'' SEAD 3 requires reporting by all contractor cleared personnel who have been granted eligibility for access to classified information. This NISPOM rule provides for a single nation-wide implementation plan which will, with this rule, include SEAD 3 reporting by all contractor cleared personnel to report specific activities that may adversely impact their continued national security eligibility, such as reporting of foreign travel and foreign contacts. NISP Cognizant Security Agencies (CSAs) shall conduct an analysis of such reported activities to determine whether they pose a potential threat to national security and take appropriate action. Finally, the rule also implements the provisions of Section 842 of Public Law 115–232, which removes the requirement for a covered National Technology and Industrial Base (NTIB) entity operating under a special security agreement pursuant to the NISP to obtain a national interest determination as a condition for access to proscribed information.

DATES: *Effective date:* This rule is effective February 24, 2021. Comments must be received by February 19, 2021.

ADDRESSES: You may submit comments, identified by docket number and/or Regulatory Information Number (RIN) and title, by any of the following methods:

- *Federal Rulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Mail:* DoD cannot receive written comments at this time due to the COVID–19 pandemic. Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number or RIN for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Valerie Heil, 703–692–3754.

SUPPLEMENTARY INFORMATION:

I. Overview of the NISP and NISPOM

In April 1990, President George Bush directed the National Security Council to explore the creation of a single, integrated industrial security program to improve security protection and provide cost savings. Prior to this, contractors doing business with different U.S. Government (USG) agencies which required access to classified information had to meet different requirements to protect the same levels of classified information, *e.g.,* the type of safe to protect a specific classified item could vary across both contracts and agencies. The diversity of industrial security requirements levied on contractors by an estimated 21 USG agencies created a significant burden on both industry and government and increased the cost of the goods and services provided to the USG.

Representatives from government and industry participated in an initiative which led to the creation of Executive Order (E.O.) 12829 ''National Industrial Security Program (NISP)'' (available at *https://www.archives.gov/files/isoo/policy-documents/eo-12829-with-eo-13691-amendments.pdf*). With the National Security Council providing overall policy direction, this E.O. established the NISP as the single integrated program to protect classified information and preserve our Nation's economic and technological interests. Nothing in the E.O. shall supersede the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended, or the authority of the Director of National Intelligence (or any Intelligence Community element) under the Intelligence Reform and Terrorism Prevention Act of 2004, the National Security Act of 1947, as amended, or Executive Order No. 12333 of December 8, 1981, as amended, or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under Executive Order 13549 of August 18, 2010 (Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities). The Information Security Oversight Office (ISOO), a component of the National Archives and Records Administration (NARA), was tasked with overseeing overall implementation of the NISP with the goal of:

- Holding classification activity to the minimum necessary to protect the national security;
- ensuring the safeguarding of classified national security information in both USG and industry in a cost-effective and efficient manner; and
- promoting declassification and public access to information as soon as national security considerations permit.

ISOO issues implementing directives and produces an annual report to the President on the NISP. E.O. 12829 also established the National Industrial Security Program Policy Advisory Committee (NISPPAC), a federal advisory committee comprised of both Government and industry representatives, which is responsible for recommending changes in industrial security policy. The NISPPAC, chaired by the Director of the ISOO, also advises ISOO on all issues concerning the policies of the NISP, including recommended changes to those policies, and serves as a forum to discuss policy issues in dispute. The NISPPAC industry members represent all types and sizes of NISP cleared entities, whose scope of operations range from a one person entity, having a single classified contract to some of the largest U.S. entities, having numerous classified contracts. All NISPPAC industry members have expertise comprising the primary functions of an industrial security program, to include information, personnel, physical, and information system security.

Five USG executive branch agencies—DoD, DOE, the Nuclear Regulatory Commission (NRC), the Office of the Director of National Intelligence (ODNI), and the Department of Homeland Security (DHS)—have been designated as Cognizant Security Agencies (CSAs) and have specific responsibilities within the NISP. For DoD, the Defense Counterintelligence and Security Agency (DCSA) is the Cognizant

Security Office (CSO) for DoD Components and non-DoD agencies where an industrial security agreement is in place. DCSA, as the DoD CSO, DOE, and NRC each has the following responsibilities:

- Administers the NISP.
- provides security oversight.
- conducts security review actions.
- provides security education and training.
- provides supplementary procedures for unique mission requirements (*e.g.* DoD publishes industrial security letters (ISLs), which provide DoD-specific guidance and clarification on NISP policies and supplementary procedures to its unique CSO mission requirements (available at: *https://www.dcsa.mil/mc/ctp/tools/*)).
- assesses, authorizes and oversees contractor information systems used to process classified information.
- makes temporary national security eligibility determinations pursuant to SEAD 8, Temporary Eligibility (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-8_Temporary_Eligibility_U.pdf*), for contractor personnel who require access to classified information.

DHS receives NISP industrial security services from DoD due to its industrial security services agreement and also has the following responsibilities:

- Prescribes procedures for the portions of this rule that pertain to the CCIPP.
- retains authority over access to information under the CCIPP.
- inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to CCIPP.

ODNI has the following responsibilities:

- Prescribes procedures for the portions of this rule pertaining to intelligence sources, methods, and activities, including, but not limited to, SCI.
- retains authority over access to intelligence sources, methods, and activities, including SCI.
- provides guidance on the security requirements for intelligence sources and methods of information, including, but not limited to, SCI.

DOE and NRC provide similar industrial security oversight actions, including national security eligibility determinations for contractor personnel, authorization of contractor information systems to process classified information, as well as monitoring and inspecting those contractors under DOE or NRC security cognizance, respectively. In 2004, the Intelligence Reform and Terrorism Prevention Act (IRTPA) (Pub. L. 108–458) created the position of the Director of National Intelligence (DNI) and recognized the ODNI as a CSA. E.O. 13691 ''Promoting Private Sector Cybersecurity Information Sharing,'' February 13, 2015 (available at *https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing*), amended E.O. 12829 to make DHS the fifth CSA in 2015.

II. NISP Implementation

DoD is the Executive Agent of the NISP and has the largest NISP contractor population of the five CSAs. DCSA inspects and monitors cleared entities, also referred to as contractors, who require access to classified information during all phases of the contracting, licensing, and grant (hereinafter referred to as contracting or contract) process to include the preparation and submission of bids and proposals, negotiation, award, performance, and termination. It also determines eligibility for access to classified information for contractors performing on classified contracts with DoD and with those USG agencies which have an industrial security agreement with DoD. The Department currently has industrial security agreements with 33 agencies (list available at: *https://www.dcsa.mil/mc/ctp/nisp/*). DCSA field elements provide oversight of contractor compliance, authorize contractor information systems to process classified information, and conduct security review actions for approximately 12,500 cleared contractor entities which includes headquarters, divisions, subsidiaries and branch offices of industrial, educational, commercial, or other non-USG entities which are performing on classified contracts.

Under the NISP, the USG establishes requirements for the protection of classified information to be safeguarded in a manner equivalent to its protection within the executive branch of USG, where practicable. When bound by contract, industry must comply with the NISPOM and any CSA-specific supplementary guidance for unique CSA mission requirements. Industry implements those requirements for the protection of classified information with advice, assistance, and oversight from the applicable CSA.

When a Government Contracting Activity (GCA), an element of an agency that has authority regarding acquisition or grant functions, awards a contract that has been determined to require access to classified information, the contract is considered to be a ''classified contract.'' The GCA checks with its applicable CSA to determine if the awarded legal entity already has an entity eligibility determination (also referred to as a facility security clearance (FCL)). GCAs will ordinarily include enough lead-time in the acquisition cycle to accomplish all required security actions. In many instances, advanced planning can ensure that access to classified information will not be required in the pre-award process. This would preclude processing an entire bidder list for FCLs. When access to classified information is not a factor in the pre-award phase, but will be required for contract performance, only the successful bidder or offeror will be processed for an FCL.

Before an entity can have access to classified information during its contract performance, it must have an FCL. If the legal entity does not already have an FCL when awarded a classified contract, a GCA must sponsor the entity for an FCL. Or, an entity already part of the NISP (*i.e.,* a prime contractor) may sponsor another entity in order to subcontract part of its classified business. To sponsor an entity, the GCA or prime contractor puts in a request, often referred to as a sponsorship letter, to the appropriate CSA for the entity to access classified information in connection with a legitimate government requirement, which may include a foreign government requirement.

With an approved FCL, an entity is then eligible for access to information classified at the level of the FCL (*i.e.,* TOP SECRET, SECRET or CONFIDENTIAL) when competing for a classified contract. Among other requirements, an entity must have sponsorship based on a valid government requirement for access to classified information. The USG agency sponsoring an entity for an FCL must include the applicable security requirements clause or equivalent in the contract (*e.g.*, for DoD this is the Federal Acquisition Regulation (FAR) 52.204–2 ''Security Requirements,'' or the terms and conditions of a grant award under 2 CFR part 200.210) to require compliance with the NISPOM.

A GCA provides the security requirements for a classified contract in a contract security classification specification as part of the contract. For DoD, the DD form 254, ''Department of Defense Contract Security Classification Specification,'' OMB Control number 0704–0567, is part of the classified contract and provides the contractor (or a subcontractor) with security requirements and the classification

guidance necessary to execute a specific classified contract. See *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254.pdf* and available at *https://www.dcsa.mil/is/nccs/*) for the current version of this collection. A contract security classification specification with its attachments, supplements, and incorporated references, provides security classification guidance (lists the applicable security classification guides for a contractor to use) to a contractor in connection with a classified contract. It is designed to identify the classified areas of information involved in the classified effort and, particularly, to identify the specific items of information within these areas that require protection. This rule provides NISP contractors security requirements which align to 32 CFR part 2001, in a manner equivalent to the protection of classified information within the executive branch of the USG. If a GCA determines that additional safeguards are essential in specific contracts, the GCA can impose more operational security provisions above the requirements of this rule. The GCA can also determine that additional physical or technical security requirements are needed in a contract above the requirements of this rule. Even though the contract security classification is contract-specific, it is not always all-inclusive. Additional security requirements are sometimes included in other parts of a contract. All related materials for approved information collection are available at: *https://www.reginfo.gov/public/do/PRAMain.* In addition, specific locations for finalized collection instruments, to include the designated OMB Control Number is included where information collections are cited in this rule.

In addition, depending upon the CSA with security cognizance, an entity's legal headquarters may need to implement additional information collections, such as:

- DD Form 441, ''DoD Security Agreement'' for DoD is an agreement between DCSA and the cleared legal entity for the entity to comply with the NISPOM security requirements, to be subject to inspections and to allow for a 30 day notice by the entity or DCSA to terminate the agreement (*e.g.,* if there is no longer a valid USG requirement for access to classified information (available at *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0441_2020.pdf*);
- NRC Form 441, ''Security Agreement'' for NRC, the provisions of the NRC Form 441 are similar to those included in the DD Form 441 (available at *https://www.nrc.gov/reading-rm/doc-collections/forms/nrc441info.html*).
- DOE does not have a separate Form 441, but instead, binds the contractor to the FCL (and security requirements) via the contract, along with meeting all other requirements in this rule.

As part of FCL processing, an entity must complete a Standard Form (SF) 328, ''Certificate Pertaining to Foreign Interest,'' OMB Control number 0704–0579, (available at *https://www.gsa.gov/forms-library/certificate-pertaining-foreign-interests,* for a CSA to review and make a determination whether the entity is under foreign ownership, control or influence (FOCI) to a degree that renders it ineligible for an FCL. The CSA will consider a U.S. entity to be under FOCI when a foreign interest has the power to direct or decide issues affecting the entity's management or operations in a manner that could either result in unauthorized access to classified information; or adversely affect performance of a classified contract or agreement. The U.S. entity may also be considered to be under FOCI when a foreign interest or government is currently exercising, or could exercise, that power, whether directly or indirectly, such as through ownership of the U.S. entity's securities, by contractual arrangements, or other means. Further, if a foreign interest or government has the ability to control or influence the election or appointment of members of the entity's governing board, the entity may be considered to be under FOCI. When a CSA has determined that an entity is under FOCI, the primary consideration will be the protection of classified information. The CSA will take whatever action is necessary to protect classified information, in coordination with other affected agencies as appropriate. A U.S. entity that is in process for an FCL for access to classified information and subsequently determined to be under FOCI, is ineligible for access to classified information unless and until effective security measures have been put in place to negate or mitigate FOCI to the satisfaction of the CSA.

Once an entity becomes a contractor in the NISP with an existing FCL, a GCA can select and award a classified contract to the entity as part of the acquisition process. The GCA attaches the ''Contract Security Classification Specification: (*e.g.,* for DoD, it is the DD Form 254, available at *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254.pdf* and available at *https://www.dcsa.mil/is/nccs/*), to all such contracts requiring access to classified information.

II. SEAD 3 Requirements and the NISPOM

In 2008, with the publication of E.O. 13467, ''Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information'' (available at *https://obamawhitehouse.archives.gov/the-press-office/2016/09/29/executive-order-amending-executive-order-13467-establish-roles-and*), the DNI was assigned the role of the Security Executive Agent (SecEA), for the development, implementation, and oversight of effective, efficient, and uniform policies and procedures governing the conduct of investigations and adjudications for eligibility for access to classified information and eligibility to hold a sensitive position.

In December 2016, the SecEA issued SEAD 3, ''Reporting Requirements for Personnel with Access to Classified Information or Who Hold a Sensitive Position'' (available at *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf*), to executive branch agencies or covered individuals with an effective date of June 12, 2017. SEAD 3 defines covered individuals as:

- A person who performs work for or on behalf of the executive branch who has been granted access to classified information or holds a sensitive positions, but does not include the President or the Vice President.
- a person who performs work for or on behalf of a state, local, tribal, or private sector entity, as defined in E.O. 13549, who has been granted access to classified information or holds a sensitive position, but does not include duly elected or appointed governors of a state or territory, or an official who has succeeded to that office under applicable law; and
- a person working in or for the legislative or judicial branches who has been granted access to classified information or holds a sensitive position and the investigation or determination was conducted by the executive branch, but does not include members of Congress, Justices of the Supreme Court, or Federal judges appointed by the President.
- covered individuals are not limited to government employees and include all persons, not excluded under paragraphs D.5(a), (b), or (c) of SEAD 3, who have access to classified information or who hold sensitive positions, including, but not limited to, contractors, subcontractors, licensees, certificate holders, grantees, experts,

consultants, and government employees.

SEAD 3 identifies required reporting of data elements that are contained in the Standard Form-86, ''Questionnaire for National Security Positions'' (available at *https://www.opm.gov/forms/pdf_fill/sf86.pdf*), which applicants and clearance holders complete during the initial and periodic reinvestigation processes, respectively. SEAD 3 requires these elements to be reported prior to participation in such activities or otherwise as soon as possible following the start of their involvement. Most notably, SEAD 3 requires covered individuals to obtain prior agency approval before conducting unofficial foreign travel.

For this rule, SEAD 3 applies only for those contractor personnel who have been granted eligibility for access to classified information through the NISP. In accordance with paragraph E.4 of SEAD 3, NISP CSAs, acting on behalf of Heads of agencies or designees, for the NISP contractors under their security cognizance may determine that operational and mission needs preclude strict adherence to these reporting requirements. In those instances, a NISP CSA may provide CSA guidance to supplement unique CSA mission requirements to the contractors under its security cognizance of equivalent notification, briefing and reporting to be accomplished.

III. Requirements From Section 842 of Public Law 115–232

Currently, the NISPOM and 32 CFR part 2004 require that GCAs, in coordination with the applicable CSAs and controlling agencies (ODNI for Sensitive Compartmented Information (SCI), DOE for Restricted Data (RD) or NSA for Communications Security (COMSEC)), complete a National Interest Determination (NID) before granting access to proscribed information to an entity that is owned or controlled by a foreign interest and cleared under a Special Security Agreement (SSA). The term ''proscribed information'' means information that is—

(A) classified at the level of top secret;

(B) communications security information (excluding controlled cryptographic items when un-keyed or utilized with unclassified keys);

(C) Restricted Data (as defined in section 11 of the Atomic Energy Act of 1954, as amended (42 United States Code (U.S.C.) 2014));

(D) special access program information under section 4.3 of E.O. 13526 (75 FR 707; 50 U.S.C. 3161 note) or successor order; or

(E) designated as sensitive compartmented information, as defined in Intelligence Community Directive 703, ''Protection of National Intelligence, Including Sensitive Compartmented Information'' (available at *https://www.dni.gov/files/documents/ICD/ICD%20703.pdf*).

An SSA is one of the mechanisms used by the USG to mitigate FOCI to an acceptable level as determined by the CSA. A company is considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, to direct or decide matters affecting the management or operations of that company in a manner which may result in unauthorized access to classified information or may adversely affect the performance of classified contracts. The following factors relating to a company, the foreign interest, and the government of the foreign interest are reviewed in the aggregate in determining whether a company is under FOCI:

- Record of economic and government espionage against U.S. targets
- Record of enforcement and/or engagement in unauthorized technology transfer
- The type and sensitivity of the information that shall be accessed
- The source, nature and extent of FOCI
- Record of compliance with pertinent U.S. laws, regulations and contracts
- The nature of any bilateral and multilateral security and information exchange agreements that may pertain
- Ownership or control, in whole or in part, by a foreign government.

Section 842 of Public Law 115–232 and this final rule provide that a covered NTIB entity operating under an SSA pursuant to the NISP, shall not be required to obtain a NID as a condition for access to proscribed information, effective October 1, 2020. DoD notified the DoD components and 33 non-DoD agencies with which DoD has industrial security agreements that NIDs pursuant to the provisions of Section 842 of Public Law 115–232 are no longer required as of October 1, 2020. DCSA is no longer submitting NID requests to ODNI for SCI, DOE for RD, or NSA for COMSEC, respectively that fall within the provisions of Section 842 of Public Law 115–232.

As provided for in the law, the Under Secretary of Defense for Intelligence and Security, on behalf of the Secretary, granted waivers of NIDs for those categories of proscribed information under the control of the Secretary of Defense, to 20 contractors that met the criteria in summer 2019 with the waivers expiring as of October 1, 2020, since the statute went into effect. Those contractors, pursuant to Section 842 of Public Law 115–232 had to meet the following criteria as part of the waiver determination:

(1) A demonstrated successful record of compliance with the NISP assessed by the CSA; and

(2) previously been approved for access to proscribed information as indicated in CSA FCL records.

The law is limited to ''a person that is a subsidiary located in the United States—

(A) for which the ultimate parent entity and any intermediate parent entities of such subsidiary are located in a country that is part of the national technology and industrial base (as defined in section 2500 of title 10, United States Code); and

(B) that is subject to the FOCI requirements of the NISP.''

Legal Authority for the NISP

In addition to E.O. 12829, which, establishes the NISP and requires the Secretary of Defense to issue and maintain the NISPOM, the following are other relevant authorities for the program.

- E.O. 10865 ''Safeguarding Classified Information within Industry,'' February 20, 1960, as amended (available at *https://www.archives.gov/federal-register/codification/executive-order/10865.html*), addresses the protection of classified information that is disclosed to, or developed by contractors.
- E.O. 12968, ''Access to Classified Information,'' August 2, 1995, as amended (available at *https://www.govinfo.gov/content/pkg/FR-1995-08-07/pdf/95-19654.pdf*), establishes a uniform personnel security program for individuals who will be considered for initial or continued access to classified information.
- E.O. 13526, ''Classified National Security Information,'' December 29, 2009 (available at *https://www.archives.gov/files/isoo/pdf/cnsi-eo.pdf*), prescribes a uniform system for classifying, safeguarding and declassifying national security information.
- E.O. 13587, ''Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,'' October 7, 2011 (available at *https://www.govinfo.gov/app/details/CFR-2012-title3-vol1/CFR-2012-title3-vol1-eo13587*), directs structural reforms to ensure responsible sharing and safeguarding of classified information on computer networks consistent with

appropriate protection for privacy and civil liberties.

• E.O. 13691; Promoting Private Sector Cybersecurity Information Sharing,'' February 13, 2015 (available at *https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-sharing*), encourages the voluntary formation of organizations engaged in the sharing of information related to cybersecurity risks and incidents to establish mechanisms to continually improve their capabilities and functions as well as to better allow them to partner with the Federal government on a voluntary basis.

• E.O. 12333; ''United States Intelligence Activities,'' December 4, 1981, as amended (available at *https://www.archives.gov/federal-register/codification/executive-order/12333.html,* provides general principles that in addition to and consistent with applicable laws are intended to achieve the proper balance between the acquisition of essential information and the protection of individual interests.

• Title 42 U.S.C. 2011 *et seq.* (also known as and referred to in this rule as ''The Atomic Energy Act of 1954,'' as amended (AEA));

• Title 50 U.S.C. chapter 44 (also known as ''The National Security Act of 1947, as amended);

• Title 50 U.S.C. 3501 *et seq.* (also known as ''The Central Intelligence Agency Act of 1949,'' as amended);

• Public Law 108–458 (also known as the ''Intelligence Reform and Terrorism Prevention Act of 2004''), which includes development of uniform and consistent policies and procedures to ensure effective, efficient and timely completion of security clearances.

• Finally, 32 CFR part 2004 ''National Industrial Security Program,'' May 7, 2018, establishes uniform standards for the NISP, and helps agencies implement requirements in E.O. 12829, and establishes agency responsibilities for implementing the insider threat provisions of E.O. 13587.

III. Changes Made by This Rule and Expected Impact

The NISPOM was first published in 1995 as DoD Manual 5220.22. Updates to the NISPOM have included Conforming Change 1, March 28, 2013 and NISPOM Change 2 in May 21, 2016. The most current version of the NISPOM (Change 2) is available at *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/522022M.pdf?ver=2019-06-06-145530-170.* In addition to codifying the NISPOM in the CFR and adding the requirements of SEAD 3 and Section 842 of Public Law 115–232, DoD is also removing 32 CFR part 117, subpart C, ''National Industrial Security Program'' because it is duplicative of 32 CFR part 2004, ''National Industrial Security Program'' and removing 32 CFR part 117, subpart B, because it is also duplicative of other industrial security provisions set forth in 32 CFR part 2004. These administrative removals support a recommendation from the DoD Regulatory Reform Task Force created under E.O. 13777, Enforcing the Regulatory Reform Agenda (available at *https://www.govinfo.gov/content/pkg/FR-2017-03-01/pdf/2017-04107.pdf*), and by themselves create no changes in current DoD policy. Upon the effective date of 32 CFR part 117, DoD will no longer publish the DoD Manual 5220.22, NISPOM as a DoD policy issuance.

Specific changes in this rule that are not in the current NISPOM, include the following.

• *§ 117.8: Reporting Requirements. § 117.8(a) General* includes that contractors must submit reports pursuant to this rule, SEAD 3 and CSA guidance to supplement unique CSA mission requirements. SEAD 3 reporting establishes a single nationwide implementation plan for covered individuals, which for this rule provides reporting by contractors and their employees eligible for access to classified information. SEAD 3 requirements will be implemented for all contractor cleared personnel to report specific activities that may adversely impact their continued national security eligibility. Contractor cleared personnel must be aware of risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the United States and abroad, and have a responsibility to recognize and avoid personal behaviors and activities that adversely affect their national security eligibility. NISP CSAs shall conduct an analysis of such reported activities, such as foreign travel or foreign contacts, to determine whether they pose a potential threat to national security and take appropriate action. Contractors will be responsible for collecting the foreign travel data from cleared employees, providing pre- and post-travel briefings to those cleared employees when necessary, and tracking and reporting those foreign travel activities of its cleared employees through the CSA designated system of record for personnel security clearance data.

• *§ 117.9(m) Limited entity eligibility determination (Non-FOCI)* and, *§ 117.11(e) Limited entity eligibility determination due to FOCI.* In accordance with 32 CFR part 2004, ''NISP Directive,'' provisions for granting two new types of limited entity facility clearance eligibility determinations (FCLs) to meet government requirements for narrowly scoped requirements for a companies to access classified information.

• *§ 117.11(d)(2)(iii)(A) Requirement for National Interest Determinations (NIDs):* This paragraph provides for the implementation of the provisions of Section 842 of Public Law 115–232, which was effective on October 1, 2020, and eliminates requirements for a covered NTIB entity operating under an SSA to obtain a NID for access to proscribed information: Top Secret, Special Access Program, Communications Security, Sensitive Compartmented Information, and Restricted Data. This provision will allow covered NTIB entities to begin performing on contracts that require access to proscribed information without having to wait on a NID, and thus removing costly contract performance delays.

• *§ 117.15(e)(2) TOP SECRET Information:* Permits specific determinations by a CSA with respect to requirements for TOP SECRET accountability (*e.g.,* the CSA can determine that TOP SECRET material stored in an electronic format on an authorized classified information system does not need to be individually numbered in series provided the contractor has in place controls in place to address accountability, need to know and retention). As stated in this paragraph: ''. . . Contractors will establish controls for TOP SECRET information and material to validate procedures are in place to address accountability, need to know and retention, *e.g.,* demonstrating that TOP SECRET material stored in an electronic format on an authorized classified information system does not need to be individually numbered in series. These controls are in addition to the information management system and must be applied, unless otherwise directed by the applicable CSA, regardless of the media of the TOP SECRET information, to include information processed and stored on authorized information systems. Unless otherwise directed by the applicable CSA, the contractor will establish the following additional controls . . .''

• *§ 117.15(d)(4) Installation:* Clarifies that an Intrusion Detection System (IDS) shall be installed by a Nationally Recognized Testing Laboratory (NRTL)-approved entity to make it clear that any NRTL-approved entity may do such

installations. ''The IDS will be installed by a NRTL-approved entity or by an entity approved in writing by the CSA . . .''

• *§ 117.7(b)(2) Senior Management Official:* Clarifies responsibilities of the Senior Management Official of each cleared entity to better reflect the critical role and accountability of this position for entity compliance with the NISPOM. This change further emphasizes the essential role of the Senior Management Official with the entity's security staff to ensure NISPOM compliance.

• *§ 117.13(d)(5)* Clarifies to the contractor that upon completion of a classified contract, the ''contractor must return all government provided or deliverable information to the custody of the government. Such clarification ensures the contractor is not retaining official government records without specific authorization from the government customer. ''(i) If the GCA does not advise to the contrary, the contractor may retain copies of the government material for a period of 2 years following the completion of the contract. The contract security classification specification, or equivalent, will continue in effect for this 2-year period. (ii) If the GCA determines the contractor has a continuing need for the copies of the government material beyond the 2-year period, the GCA will issue a final contract security classification specification, or equivalent, for the classified contract and will include disposition instructions for the copies.''

Costs

The DoD invites comment from the members of the public on the costs estimated to implement this rule.

A. Baseline

The Defense Counterintelligence and Security Agency (DCSA), as the DoD designated NISP cognizant security office, has collected information about baseline costs using an OMB-approved information collection process employing statistical methods for contractors' NISP implementation (OMB Control Number 0704–0458, ''Industry Cost Collection Report Survey.'' The most recent data collected by DCSA on contractors' NISP implementation costs are for fiscal year (FY) 2017 and reported in the ISOO 2017 annual report to the President. DCSA has used this survey collection methodology for contractors' NISP implementation under DoD security cognizance for over 11 years. A NISP government and industry working group developed the survey in 1995 and predecessor office to the OUSD(I&S) initially ran the annual survey. The Information Security Oversight Office (ISOO) placed a moratorium on conducting this survey after 2017 until a new NISP survey methodology is developed.

DCSA began the costs analysis for the baseline costs for fiscal year 2017 by randomly selecting active NISP contractor facilities that have existing DoD approval for classified storage at their own physical locations and having those facilities submit security costs. The randomly selected contractor facilities also have an active facility security clearance and a permanent Commercial and Government Entity (CAGE) Code. In addition to the randomly selected cleared facilities having approved classified storage, DCSA categorizes these contractor facilities for the survey based on the size, scope, and complexity of each contractor's security program.

The general methodology used to estimate security costs incurred by contractor cleared facilities with approved storage of classified information is based on the costs incurred by respondent contractors for the protection of classified information. The methodology captures the most significant portion of industry's costs, which is labor. Security labor in the survey is defined as personnel whose positions exist to support operations and staff in the implementation of government security requirements for the protection of classified information. Guards who are required as supplemental controls are included in security labor. The respondent contractors are requested to compile their cleared facility's current annual security labor cost in burdened, current year dollars with the most recent data being from the 2017 survey. The labor cost, when identified as an estimated percent of each contractor's total security costs, enables the respondent contractors to calculate their total security costs.

Information collected is compiled to create an aggregate estimated cost of NISP classification-related activities. Only the aggregate data is reported. There is a 95% confidence that the full enterprise industrial security total baseline cost does not exceed $1.486 billion for fiscal year 2017.

NISP cost estimates (2017)	Benefits of NISP rule
Number of Facilities with Approved Classified Storage (Of Over 12,000 NISP Cleared Facilities):	
3658	A single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests.
Facilities Randomly Selected and Responding to Data Collection:	
1038	Maximum uniformity and consistency by contractors who support the Executive branch to effectively protect and safeguard classified information through all phases of the contracting process for any classified information an Agency releases to a contractor.
Estimated Total NISP Security Costs for Facilities with Approved Classified Storage (With 95% Margin of Error to give 95% Upper Confidence Limit):	
$1,413,150,249 + $72,968,977 = $1,486,119,226	Contractors must comply, when levied by the FAR security requirements clause or equivalent clauses in contracts involving access to classified information, with uniform procedures for the proper safeguarding of classified information to reduce the risk of unauthorized disclosure of classified information.

Based on the data collected from the survey, we can be 95% confident the true 2017 total NISP security cost for contractor facilities with approved classified storage is less than $1.486B.

Assumptions and Notes:

• Of over 12,000 NISP cleared facilities, 3,658 facilities are approved for classified storage and 1,038 responded to the survey.

- Companies were selected at random according to survey methodology.
- The applicable NISP CSA, based on a valid requirement for access to classified information (*e.g.,* contract or bid), funds the costs for evaluating and processing a contractor for an entity eligibility determination (facility clearance) and the costs of personnel security vetting requirements for required access to classified information by any contractor employees.
- The security cost profile for non-responding companies is assumed to be similar to that of responding companies.
- Outlying survey data points were removed from data analysis.
- Overall DoD contract spending for 2017 was $331 billion; but DoD does not have such data for these contractor cleared facilities in the NISP for performance on contracts requiring access to classified information.
- DoD has not collected security costs from those contractor cleared facilities that are not authorized to store classified information at their own contractor locations.

DoD noted that the largest contractor cleared facilities account for the highest security costs, and skew the average security costs for non-small businesses much higher. The average security cost for the largest contractor cleared facilities is approximately $4.8 million per facility. If the largest facilities are removed from the cost estimate, then the average security cost for a non-small business with approval for storage of classified information is reduced to $432,312 from $864,662. Of the approximately 1,000 facilities selected for the small entities analysis described in section 4 of this initial regulatory flexibility analysis, about 68% were contractor cleared facilities that were not included in the 2017 NISP cost estimate because they don't have approval to store classified information or process classified information on an information system or network at the contractors' own cleared facilities. DoD estimated the costs impacting small entities from the approximately 32% of the remaining small businesses, as those would have approval to store classified information or process classified information on an information system or network at one of the contractor's own cleared facilities. Those security costs are estimated to be approximately $316 million or 21% of the $1.486 billion of the estimated NISP costs to contractors in 2017. When contractor cleared facilities' responses to the ISOO cost collection survey were cross referenced with the DoD small business analysis (using the Small Business Administration (SBA) Dynamic Small Business Search), DoD estimated an average security cost for a small business with approved storage of classified information of $133,612. One of the requirements for a facility security clearance is a security agreement between the applicable NISP CSA and the contractor legal entity. Such a security agreement sets forth compliance, oversight and administration termination provisions. The agreement also indicates that it does not obligate USG funds and the USG shall not be liable for any costs or claims of the contractor arising out of the security agreement. It is recognized, however, the parties may provide in other written contracts with GCAs for security costs, which may be properly chargeable, if so determined by the applicable GCA. This rule provides that a contractor must implement changes no later than 6 months from the date of a published change to this rule to allow the contractor to discuss what impact, if any, the changes have on existing classified contracts with the applicable GCAs.

B. Public Cost Analysis of the Changes to the Baseline From This Rule

1. *Projected Public Costs.* In summary, the estimated public costs are present value costs of 150.26 million and annualized costs estimated to be $10.52 million.

2. *Cost Analysis.* Throughout, labor rates are adjusted upward by 100% to account for overhead and benefits.

a. *Regulatory Familiarization.* There will be an initial step to become familiar with the format of the rule, the changed requirements and what actions the cleared entities must take to comply with the changes in this rule. To become familiar with the rule format and the new requirements, cleared entities will review the **Federal Register** notice with the new 32 CFR part 117. It is estimated that 12,400 cleared entities will need to become familiar with the rule. Of those approximately 12,400 cleared entities, an estimated 8,036 are small business entities and 4,348 are large business entities. The FSO at each entity (small or large) must become familiar with the rule to be able to use it on a daily basis in the FSO role to supervise and direct security measures necessary for implementing the applicable security requirements to ensure the protection of classified information. Using the published Office of Personnel Management General Schedule (GS) salary schedule for fiscal year (FY) 2020, the estimated labor rate for an FSO of a small business entity firm is the equivalent of a GS11 step 5 and for an FSO of a large business entity as the equivalent of a GS13, step 5. It is estimated that it will take 10 hours in the first year, 5 hours in years 2 and 3, 3 hours in years 4 to 7, and then 2 hours annually up to year 20 for an FSO to become familiar with the rule, as this will be the first time that the NISPOM is in a rule format instead of as a DoD policy issuance, as well as familiarization with the changes. These assumptions imply costs of $9.89 million in year one; $4.95 million in years 2 and 3; $2.97 million in each year 4 through 7; and, $1.98 million in each year 8 through 20.

b. *Evaluation of Existing Classified Contracts To Implement Changes No Later than Six Months from Effective Date.*

Each of the legal U.S. cleared entities must comply no more than six months from the effective date of this NISPOM rule. During that six months, each legal cleared entity has the opportunity to review existing classified contracts to determine if there is any impact that they want to discuss with the applicable GCAs about possible equitable adjustment. Decisions on any requests for equitable adjustment will be made by the applicable contracting officer. Legal entities enter into contracts, licenses or grants; it is estimated that the average of 8,036 small business cleared entities are each a legal entity. It is estimated that each of those small business cleared legal entities will review an average of 3 existing classified contracts for possible equitable adjustment for a total of 24,108 contracts requiring 3 hours each for review in 2021. Using the published Office of Personnel Management GS salary schedule for FY20, the estimated labor rate for an FSO of a small business entity firm is the equivalent of a GS11 step 5 and for an FSO of a large business entity as the equivalent of a GS13, step 5. Of the large business entities, it is estimated that 2,100 large business cleared entities are legal entities, while the remaining large business entities are divisions or branch offices. It is estimated that each of those large business cleared legal entities will review an average of 30 existing classified contracts for possible equitable adjustment for a total of 63,000 contracts requiring 8 hours each for review in 2021. It is estimated that it will take more time for review by the

large business cleared entities due to more complicated contracts. These assumptions imply costs of $54.96 million in year one and no further costs as this action is taken only in the first year.

c. *Train SECRET cleared employees on requirements to submit foreign travel reports.* The FSO at each entity (small or large) must ensure that its SECRET cleared employees are trained on the requirements. Such training by the FSO is estimated to take 1 hour in 2021 and a half an hour in each of the following years up to year 20. Using the published Office of Personnel Management GS salary schedule for FY20, the estimated labor rate for an FSO of a small business entity firm is the equivalent of a GS11 step 5 and for an FSO of a large business entity as the equivalent of a GS13, step 5. These assumptions imply total costs of $0.99 million in 2021 as year one; and, $0.49 million in each year 2 through 20.

d. *Submit foreign travel reports and receive any pre-travel threat briefings or post travel briefings based on the threat.* All cleared employees must submit foreign travel reports and receive any pre-travel briefings or post travel briefings from the FSO-based on threat according to this rule, SEAD 3 and CSA-provided guidance for unique mission requirements. It is estimated that the number of foreign travel reports submitted annually will be 483,681 to comply with this rule. That estimate is based on analysis of calendar year 2019 unofficial foreign travel reported by DoD civilians and military in the DoD Aircraft and Personnel Automated Clearance System (APACS), a web-based tool for the creation, submission and approval of aircraft diplomatic clearances and personnel travel clearances (*i.e.* Country, Theater and Special Area, as applicable with individual DoD Foreign Clearance Guide (FCG), *https://www.fcg.pentagon.mil* country pages) designed to aid USG travelers on official government and unofficial (*i.e.,* leave) travel. For calendar year 2019, there were 126,131 travelers and 113,214 travel requests submitted into APACS. APACS requirements are published on the DoD Foreign Clearance Guide (FCG), *https://www.fcg.pentagon.mil.* Thus an annual estimate of .89 expected foreign travel trips by traveler (113,214 divided by 126,131). In the small business analysis, there were a total of 18,242 cleared employees in the 658 small entities sampled and 63,598 cleared employees in the remaining 356 non-small businesses. Of the total cleared employees in the small business analysis (as reported in the National Industrial Security System), approximately 22.3% were at small entities and 77.7% were at non-small businesses. Known number of new travelers expected to be effected by this rule is 543,462 SECRET cleared contractor personnel under DoD security cognizance and the estimated trips at .89 per traveler is (543,462 × .89 = 483,681 estimated trips). Assuming the ratio for those employees reporting foreign travel into APACS is the same as SECRET cleared employees would report, of the estimated 483,681 foreign trips by SECRET cleared employees, it can be estimated that approximately 107,812 (22.3% of 483,681) will be taken by contractors at small entities, and 375,869 (77.7% of 483,681) by contractors at non-small businesses. It is estimated that it will take a half an hour for a SECRET cleared employee to report foreign travel in 2021 and in each of the following years up to year 20 to report foreign travel and receive any pre-travel or post-travel briefings. The estimated average labor rate for a SECRET cleared employee to report foreign travel is the equivalent of a GS11 step 5. These assumptions imply costs of $16.81 million in each year one through 20.

e. *Fewer contract performance delays by the small number of U.S. contractors with NTIB ownership operating under an SSA.* Section 842 of Public Law 115–232, is limited to a small number of U.S. cleared legal entities in the NISP for which the ultimate parent entity and any intermediate parent entities of such subsidiary are located in a country that is part of the NTIB; and that is subject to the FOCI requirements of the NISP. There are currently 20 U.S. cleared legal entities with their associated cleared divisions, subsidiaries or branch (estimated to be another 100 cleared entities) to whom Section 842 of Public Law 115–232 applies. Section 881 of Public Law 114–328 expanded the legal definition of the NTIB to include the United Kingdom and Australia. The NTIB is comprised of the United States, the United Kingdom of Great Britain and Northern Ireland, Canada and Australia. NTIB is based on the principle that defense trade between the United States and its closest allies enables a host of benefits, including increased access to innovation, economies of scale, and interoperability (10 U.S.C. 2500).

Section 842 of Public Law 115–232 is deregulatory by statute and this rule. There are no estimated costs to the small number of entities impacted because they are required already to submit any new or change to FOCI information for their initial and continued FCL, respectively, via the SF 328, Certificate Pertaining to Foreign Interests in the NISP as do all other U.S. cleared legal entities. 32 CFR part 2004 provides a CSA up to 30 days to assess the submitted NID and then another 30 days for a controlling agency to make a NID for the type of proscribed information under the purview of each (ODNI for SCI, DOE for RD or NSA for COMSEC). Thus, with Section 842 of Public Law 115–232, there has been minimum 60 day delay for a NID involving an NTIB covered entity which has impacted the timeliness of contract performance. There are estimated costs savings as this small number of cleared entities and their entity cleared employees designated to work on specific classified contracts involving proscribed information will no longer have to wait at least 60 days for NIDs after contract award for access to proscribed information when all other requirements have been met for access to classified information and contract performance. Using the published Office of Personnel Management GS salary schedule for FY20, the labor rate for an FSO and an estimated 8 cleared employees in each of the 2 small business entities impacted is the equivalent of a GS11 step 5 with a time savings of 320 hours for each year 1 through 20. The labor rate for an FSO and an estimated 19 cleared employees in each of the 18 large business entities impacted is the equivalent of a GS13 step 5 with a time savings of 320 hours for each year 1 through 20. These assumptions imply cost savings of $11.81 million in each year.

C. USG Cost Analysis of the Changes to the Baseline From This Rule

1. *Projected USG Cost/Cost Savings.* In summary, the estimated USG cost/cost savings are present value costs of $10.82 million and annualized costs of $0.76 million. Throughout, labor rates are adjusted upward by 100% to account for overhead and benefits.

2. *Cost analysis.*

a. Regulatory Familiarization. There will be an initial step to become familiar with the clause requirements and what actions the USG executive branch agencies must take to comply with the changes in this rule. To become familiar with the new requirements, USG executive branch agencies may review the **Federal Register** notice with the new 32 CFR part 117. It is estimated that 38 USG executive branch agencies will become familiar with the rule (*i.e.,* the five Cognizant Security Agencies (DoD, DOE, NRC, ODNI, DHS) and the 33 USG agencies which currently have an industrial security services agreement

with DoD pursuant to 32 CFR part 2004). The estimated labor rate used for the cost calculation is the equivalent of a GS12 step 5 for the designated NISP lead at each of those 38 agencies. It is estimated that it will take 8 hours in the first year as well as in each of the following through year 20 to become familiar and remain familiar with the rule, as this will be the first time that the NISPOM is in a rule format instead of as a DoD policy issuance, as well as familiarization with the changes. These assumptions imply costs of approximately $25 thousand each year.

b. *Training the USG civilian employees of NISP CSAs who provide oversight of contractor compliance with this rule.* It is estimated that the NISP CSAs (*i.e.,* DoD, DOE, NRC, ODNI and DHS) must train a total of 800 personnel who provide oversight of contractor compliance with this rule in the first year with annual refresher training in subsequent years. The largest number of personnel would be trained by DoD. The initial training is estimated to take 24 hours in 2021 to ensure those government personnel conducting oversight are versed in the changed requirements to assess compliance by cleared entities. The second year refresher training will be 16 hours with 8 hours of refresher training in each of years 3 through 20. The average labor rate for these 800 government headquarters and field personnel is estimated to be a GS13 step 5. These assumptions imply costs of $1.90 million in year one; $1.27 million in year 2; and, $0.63 million in each year 3 through 20.

c. *Accepting submissions of foreign travel reports by SECRET cleared entity personnel.* DoD, with the largest population of cleared entity personnel, already has the data fields for foreign travel reporting in the Defense Information System for Security and will not have to make more changes to that automated system to accept submission of these reports. There are no expected costs or costs savings.

d. *No longer draft, coordinate and submit proposed national interest determinations (NIDs) for access to proscribed information for the small number of U.S. contractors with NTIB ownership operating under an SSA.* There will be a small cost savings because DoD Components (*i.e.,* Departments of the Army, Navy and Air Force, DARPA, DIA, NGA, NRO, NSA and assorted smaller organizations) will no longer have to take an estimated 40 hours a year to draft, coordinate and submit NIDs for the small number of U.S. contractors with NTIB ownership operating under an SSA. There will be minimal administrative changes to the DoD information system to remove the NID requirement for the small number of NTIB covered entities. DoD already must evaluate any changes submitted to FOCI information for U.S. cleared legal entities under its security cognizance which would include a determination if one of these cleared legal entities remains a covered NTIB entity. On average, DoD receives an estimated one FOCI changed condition report annually from an NTIB covered cleared legal entity. An estimated 10 government personnel with an estimated labor rate of a GS11 step 5 would save 40 hours in year 1 through year 20. These assumptions imply costs saving of approximately $28 thousand each year.

e. *Update training materials, job aids and associated tools for U.S. cleared legal entities and USG agencies on these changes to the NISPOM.* CSAs will have to update existing training materials and products used by U.S. cleared legal entities and USG agencies so that they have all needed information on the changes being implemented in this NISPOM rule. Examples of those training materials and products range from online or in person training, job aids and web tools. DoD provides NISP training materials to the largest population, to include USG agencies and U.S. cleared legal entities, and estimates the time impact in year one is 1,128 hours for each of six individuals to update all the training materials with 564 hours in year two and 282 hours each year for maintenance of those materials in year 3 through year 20. The labor rate for those 6 personnel is estimated to be a GS13 step 5. These assumptions imply costs of $0.67 million in year one; $0.34 million in year 2; and $0.17 million in each year 3 through 20.

C. Total Costs/Cost Savings

In summary the estimated public and USG costs/cost savings are (1) present value costs of $150.26 million and annualized costs of $10.52 million for the public; and, (2) present value cost of $10.82 million and annualized costs of $0.76 million for the USG. Throughout, labor rates are adjusted upward by 100% to account for overhead and benefits.

Benefits

Following the September 2013 Navy Yard shooting, the President directed the Office of Management and Budget (OMB) to lead a review of suitability and security clearance procedures for Federal employees and contractors (see *https://www.archives.gov/files/isoo/oversight-groups/nisp/2014-suitability-and-processes-report.pdf*). This review assessed USG policies, programs, processes, and procedures involving determinations of federal employee suitability, contractor fitness, and personnel security. The interagency working group also evaluated the collection, sharing, processing, and storage of information used to make suitability, credentialing, and security decisions. It found the need for

- better information sharing,
- increased oversight over background investigations, and
- consistent application of standards and policies for both Federal employees and contractors.

The report identified 13 recommendations to improve how the Government performed suitability determinations and security clearances and the creation of SEAD 3 is a partial response to recommendation A.2. SEAD–3 requires enhanced additional reporting of foreign travel, foreign contacts and conduct/behavior that might jeopardize an individual from maintaining access or eligibility to access classified information. Many of the requirements are a direct result of recent national security breaches by trusted insiders who have disclosed classified information to news media or foreign entities causing significant harm to the interests of the United States.

SEAD 3 was designed to strengthen the safeguarding of national security equities, such as national security information, personnel, facilities, and technologies. These reporting requirements are important because individuals who incur a continuing security obligation need to be aware of the risks associated with foreign intelligence operations and/or possible terrorist activities directed against them in the U.S. and abroad, and to be aware they possess or have access to information that is highly sought after by foreign adversaries and competitors, including, but not limited to:

- Classified or sensitive information vital to national and economic security
- Emerging technologies and pioneering research and development
- Information relating to critical infrastructure sectors
- Proprietary secrets
- Security or counterintelligence information

In particular, the risk of becoming an intelligence target increases greatly during foreign travel, be it for official or unofficial purposes. NISP Contractor cleared personnel can become the target of a foreign intelligence or security service at any time in any country.

Collecting additional information on travel will help ensure basic counterintelligence awareness is implemented to effectively protect both the individual and the USG against foreign attempts to collect sensitive, proprietary, or classified information. Such measures could include arranging a pre-travel briefing from the entity Facility Security Officer. Reminders include, but are not limited to the following, which can be provided to:

- Do not leave items that would be of value to a foreign intelligence service unattended in hotel rooms or stored in hotel safes.
- Limit sensitive discussions—hotel rooms or other public places are not suitable locations to discuss sensitive information.
- Not use computer or facsimile equipment at foreign hotels or business centers for sensitive matters.
- Not divulge information to anyone unauthorized to hear it.
- Ignore or deflect intrusive inquiries or conversation about business or personal matters.
- Keep a laptop computer as carry-on baggage—never check it with other luggage and, if possible, remove or control storage media. Confirm before the foreign travel whether it is necessary or even advisable to take a laptop computer.
- Report any suspicious contacts or incidents to the entity FSO to report to the applicable CSA.

Contractors in the NISP also have a responsibility for recognizing and avoiding personal behaviors and activities that may impact their continued eligibility for access to classified information. This includes, but is not limited to the following activities which may be of potential security, insider threat, or counterintelligence concern

- An unwillingness to comply with rules, regulations, or security requirements
- Unexplained affluence or excessive indebtedness
- Alcohol abuse
- Illegal use or misuse of drugs or drug activity
- Apparent or suspected mental health issues where there is reason to believe it may impact the individual's ability to protect classified information or other information prohibited by law from disclosure
- Criminal conduct
- Any activity that raises doubts as to whether the individual's continued national security eligibility is clearly consistent with national security interests
- Misuse of U.S. Government property or information systems

This rule will result in fewer contract performance delays by the small number of U.S. contractors with NTIB ownership operating under an SSA. With Section 842 of Public Law 115–232 implemented there will no longer be at least a 60 day minimum delay for USG contracting activities and NTIB covered entities to wait for NIDs after contract award for access to proscribed information when all other requirements have been met. When a GCA submits a NID to the applicable CSA, there is an initial 30 days to process the request, which includes verification of the NID requirement. If the NID also includes a requirement for controlling agency concurrence (*i.e.,* ODNI for SCI, DOE for RD or NSA for COMSEC), the CSA submits the request to the applicable controlling agencies who then have 30 more days for its analysis and decision. Section 842 of Public Law 115–232 is deregulatory by statute as reflected in this rule. Congress required that the NTIB policy framework foster a defense free-trade area among the defense-related research and development sectors of the United States, Canada, Australia and the United Kingdom. Section 881 of Public Law 114–328 (the National Defense Authorization Act for Fiscal Year 2017) expanded the legal definition of the NTIB to include the United Kingdom and Australia. Congress expanded the NTIB in 2017 based on the principle that defense trade between the United States and its closest allies enables a host of benefits, including increased access to innovation, economies of scale, interoperability, and to reduce the barriers to the seamless integration between the NTIB which supplies defense articles to the Armed Forces and enhances allied interoperability of forces. Section 842 of Public Law 115–232 also continues the congressional intent to remove barriers to the seamless integration of the transfer of knowledge, goods, and services among the persons and organizations of the NTIB for national security challenges across a variety of technology areas.

Alternatives

No action. If there were no action (*i.e.,* no NISPOM rule nor DoD Manual 5220.22), USG agencies would not have single set of requirements to be levied on contractors through a FAR security requirements clause or equivalent to protect classified information in contracts. Without that single set of requirements consistently levied for classified contracts by USG agencies, there would be a loss of classified information to adversaries. There would not be a streamlined process for clearing contractors to work on contracts involving classified information. This would leave each USG agency to clear its own contractors, which could take months or years. The ability for the USG to fill crucial mission gaps using contractors would be severely impacted. There would be no standardized way under which contractors would be required to physically store classified information. The USG would have no insight into insider threats from contractor personnel who have access to the USG's most sensitive and critical programs. There would be an adverse impact on national security. The results of this alternative are not preferred.

Next Best Alternative. Each USG agency would establish a rule for contractor protection of classified information disclosed or released to contractors. Differing standards will result in inconsistent standards, confusion, and higher costs for compliance if a contractor has contracts requiring access to classified information with multiple USG agencies and has to comply with different agency requirements. Further, such an alternative would result in additional time needed for contractors to put in place mechanisms to meet multiple and differing sets of requirements. This inconsistency and confusion due to differing standards also increases the likelihood of loss of classified information and insider threats going undetected. The results of this alternative are not preferred.

The Preferred Alternative. This final rule provides a single statement of requirements for contractors to comply with for maximum uniformity and consistency, for the protection of classified information, to include the reporting of foreign travel and foreign contacts by cleared contractor personnel in accordance with Security Executive Agent policies. This final rule provides for the proper protection of classified information disclosed or released by U.S. agencies in all phases of the contracting, license or grant processes. This rule will prevent the theft of classified national security assets and information by adversaries and insider threats. This is the preferred alternative.

IV. Exception to Notice and Comment

This rule directly involves matters relating to public grants or contracts, and is therefore expressly exempt from notice and comment procedures under 5 U.S.C. 553(a)(2). Compliance with this rule is levied by a Federal Acquisition Regulation security requirements clause

or equivalent. It establishes requirements for the protection of classified information disclosed to or developed by contractors, licensees, grantees, or certificate holders. Industry implements these requirements to protect national security interests, cleared persons, and the integrity of the classified information. Although DoD has determined that an exception to the notice and comment requirements of § 553 applies, it still seeks public comments on this rule. Thereafter, DoD will consider comments received on this rule in determining whether to make any changes in a subsequent rule.

V. Regulatory Analysis

Executive Order 12866, ''Regulatory Planning and Review'' and E.O. 13563, ''Improving Regulation and Regulatory Review''

E.O.s 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distribute impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. Accordingly, the rule has been reviewed by the Office of Management and Budget (OMB) under the requirements of these E.O.s. This rule has been designated a significant regulatory action and determined to be economically significant, under section 3(f) of E.O. 12866 as it has an annual effect on the economy of $100 million or more or affects in a material way the economy or a sector of the economy. Security costs relate specifically to protection of classified information by cleared U.S. entities.

Executive Order 13771, ''Reducing Regulation and Controlling Regulatory Costs''

This rule is not subject to the requirements of E.O. 13771, because the rule is issued with respect to a national security function of the United States.

Public Law 96–354, ''Regulatory Flexibility Act'' (5 U.S.C. 601)

The DoD certifies that this final rule would not, if promulgated, have a significant economic impact on a substantial number of small business entities in accordance with the Regulatory Flexibility Act (5 U.S.C. 601) requirements since a contractor cleared legal entity may, in entering into contracts requiring access to classified information, negotiate for security costs determined to be properly chargeable by a GCA. The DoD invites comment from members of the public who believe there will be a significant impact.

Small entities to which this rule will apply provide products and services to the executive branch, *e.g.,* in the areas of administration, consulting, information security and technology, cybersecurity, research and development, design, production and manufacturing, including circumstances where physical security measures cannot preclude aural or visual access to classified information. These small business entities, as well as non-small business entities, have entered into a contract, license or grant for which access to classified information is required. Compliance with this rule, also referred to as the NISPOM, is levied by a FAR security requirements clause or equivalent. The requirements for an entity eligibility determination do not include USG collection of applicable North American Industry Classification System (NAICS) codes. While this type of information is available in the Federal Procurement Data System (FPDS), entity eligibility determinations (often referred to as facility clearances) are not available in FPDS. DoD has no efficient mechanism to cross check NAICS codes from FPDS with facility clearance data. DoD assesses there are a wide variety of NAICS codes associated with contracts requiring access to classified information. For example, the following NAICS codes may be associated with contracts requiring access to classified information: 561720 janitorial services; 561210 facility support services; 541611 administrative management and general management services; 561110 office administrative services; 541690 other scientific and technical consulting services; 541330 engineering services; 561611 investigation services; and likely many others, since contracts that require a facility clearance for access to classified information are not industry specific.

Based on the number of small businesses registered within the SBA Dynamic Small Business Search, the overall industrial base of federal government small businesses is 313,651. Approximately 1,000 facilities were randomly selected from the NISP to determine if the selected facilities were registered within the SBA Dynamic Small Business Search. With 95% confidence, it can be estimated that there are between 7,672 and 8,400 small entities impacted by this rule. The general methodology to determine a random sample and the estimated number of small business entities impacted by this rule is outlined in the following table. The random selection is dependent on the contractor facility having an active facility security clearance and permanent CAGE Code.

NISP small entities estimate	
Total cleared contractor facilities enrolled in the DoD National Industrial Security System (NISS) as of May 14, 2020: 12,384.	
Randomly Selected facilities from the current cleared contractor population: 1,014.	
The proportion of cleared contractor facilities in the simple random sample enrolled in the SBA Database:	
658/1,014 = 64.89%	Equates to 8,036 facilities as small business entities.
Margin of Error for proportion enrolled in SBA database (95% confidence):	
±2.94%	Equates to ±364 facilities cleared contractor facilities.
The interval estimate for the number of small businesses in the NISP:	
8,036 ±364 =	7,672 to 8,400 cleared contractor facilities.

Based on the simple random sample, we can be 95% confident that the true proportion of active cleared contractor facilities enrolled in the SBA database is between 62.0% and 67.8%. Based on cleared contractor enrollment as of May 14, 2020, the percentages equate to an interval estimate between 7,672 and 8,400 small business entities which are cleared contractor facilities and impacted by this rule.

Assumptions and Notes:

- Facilities self-enrolled in the SBA database are, in fact, small businesses. The following link was used to determine if a facility was a small business by searching CAGE codes showing all NAICS for which a business is a small business: *https://web.sba.gov/pro-net/search/dsp_dsbs.cfm.*
- The SBA database is generally a self-certifying database. The SBA does not make any representation as to the accuracy of any of the data included, other than certifications relating to 8(a) Business Development, HUBZone or Small Disadvantaged Business status. The SBA strongly recommends that contracting officers diligently review a bidder's small business self-certification before awarding a contract.
- Facilities were selected from the active NISS population using a simple random sample (1,014 selected of 12,384 enrolled facilities).
- Selection of each facility is independent of all other facilities selected (N * .10 >n).
- The sample is large enough (n = 1014) that we can assume the sampling distribution of sample proportions is approximately normal (n * p>10 and n * (1 − p) >10).

Congressional Review Act

The Congressional Review Act, 5 U.S.C. 801 *et seq.,* as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, generally provides that before a rule may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. We will submit a report containing this rule and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States. A major rule cannot take effect until 60 days after it is published in the **Federal Register**. This final rule is a ''major rule'' as defined by 5 U.S.C. 804(2) because it is also economically significant under section 3(f) of E.O. 12866 with an annual effect on the economy of $100 million or more.

Sec. 202, Public Law 104–4, ''Unfunded Mandates Reform Act''

Section 202 of the Unfunded Mandates Reform Act of 1995 (UMRA) (2 U.S.C. 1532) requires agencies to assess anticipated costs and benefits before issuing any rule whose mandates require spending in any 1 year of $100 million in 1995 dollars, updated annually for inflation. This final rule will not mandate any requirements for State, local, or tribal governments, nor will it affect private sector costs.

Public Law 96–511, ''Paperwork Reduction Act'' (44 U.S.C. Chapter 35)

It has been determined that 32 CFR part 117 does impose reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995. DoD is not proposing changes to the DoD collections based on this final rule, nor have any of the other NISP CSAs indicated proposed changes based on this rule. The DOE and NRC have collections based on their respective authorities as a NISP CSA; but neither has a collection for a Contract Security Classification Specification because DOE and NRC each complete that specification for both prime contracts and subcontracts. By accepting the contract, the contractor obligates itself to fulfill the requirements specified in applicable DOE Acquisition Regulation (DEAR) clauses (available at *https://www.energy.gov/management/downloads/searchable-electronic-department-energy-acquisition-regulation*) and identified DOE Directives. The DOE Directives contain a contractor requirements document that conveys security obligations and the statutes for civil penalties for security violations. The Nuclear Regulatory Commission Acquisition Regulation part 2052.204–70 includes the security requirements levied on the contractor (available at *https://www.acquisition.gov/nrcar/nrcar-part-2052-solicitation-provisions-and-contract-clauses#P41_1774*). For ease of review of this rule, the collections are discussed below. Materials associated with all of the collections can reviewed at *www.reginfo.gov.*

- OMB Control Number 0704–0194, DD Form 441, *DoD Security Agreement.*
- OMB Control Number: 0704–0571, *National Industrial Security System,* is a DoD information collection used to conduct its monitoring and oversight of contractors.
- OMB Control Number 0704–0567, DoD *Contract Security Classification Specification,* this collection is used by both DoD and agencies which have an industrial security agreement with DoD.
- OMB Control Number 0704–0573, *Defense Information System for Security,* is a DoD automated system for personnel security, providing a common, comprehensive medium to record, document, and identify personal security actions within DoD including submitting adverse information, verification of security clearance status, requesting investigations, and supporting continuous evaluation activities. It requires personal data collection to facilitate the initiation, investigation and adjudication of information relevant to DoD security clearances and employment suitability determinations for active duty military, civilian employees and contractors seeking such credentials.
- OMB Control Number 0704–0496, *Joint Personnel Adjudication System,* an information system which requires personal data collection to facilitate the initiation, investigation and adjudication of information relevant to DoD security clearances and employment suitability determinations for active duty military, civilian employees and contractors seeking such credentials.
- OMB Control Number 0704–0579, *Certificate Pertaining to Foreign Interests SF (328)* which is a common form which can be used by all CSAs.
- OMB Control Number 3150–0047, *10 CFR part 95, Facility Security Clearance and Safeguarding of National Security Information and Restricted Data,* is an NRC information collection used to obtain an FCL and for safeguarding Secret and Confidential National Security Information and Restricted Data. Licensees under 10 CFR part 95 fall within two categories, those who possess, use or transmit classified matter at their site or a cleared contractor site, and those licensees and contractors who only need access to classified matter at a government or appropriately cleared non-government site.
- OMB Control Number 1910–1800, *Security Package,* is a DOE information collection used by DOE to conduct its monitoring and oversight of contractors under its security cognizance and to provide a platform for other CSAs, GCAs or prime contractors to verify whether a contractor has a DOE-granted FCL.

Executive Order 13132, ''Federalism''

E.O. 13132 establishes certain requirements that an agency must meet when it promulgates an final rule (and subsequent final rule) that imposes substantial direct requirement costs on

State and local governments, preempts State law, or otherwise has Federalism implications. This final rule will not have a substantial effect on State and local governments.

List of Subjects in 32 CFR Part 117

Classified information; Government contracts; USG contracts, National Industrial Program (NISP); Prime contractor, Subcontractor.

■ Accordingly, the Department of Defense amends chapter I of title 32 of the CFR by adding part 117 to read as follows:

PART 117—NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL (NISPOM)

Sec.

Authority: 32 CFR part 2004; E.O. 10865; E.O. 12333; E.O. 12829; E.O. 12866; E.O. 12968; E.O. 13526; E.O. 13563; E.O. 13587; E.O. 13691; Public Law 108–458; Title 42 U.S.C. 2011 *et seq.*; Title 50 U.S.C. Chapter 44; Title 50 U.S.C. 3501 *et seq.*

§ 117.1 Purpose.

(a) This rule implements policy, assigns responsibilities, establishes requirements, and provides procedures, consistent with E.O. 12829, ''National Industrial Security Program''; E.O. 10865, ''Safeguarding Classified Information within Industry''; 32 CFR part 2004; and DoD Instruction (DoDI) 5220.22, ''National Industrial Security Program (NISP)'' (available at *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/522022p.pdf?ver=2018-05-01-073158-710*) for the protection of classified information that is disclosed to, or developed by contractors of the U.S. Government (USG) (hereinafter referred to in this rule as contractors).

(b) This rule, also in accordance with E.O. 12829, E.O. 13587,''Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information''; E.O. 13691, ''Promoting Private Sector Cybersecurity Information Sharing''; E.O. 12333, ''United States Intelligence Activities''; 42 U.S.C. 2011 *et seq.* (also known as and referred to in this rule as the ''AEA of 1954,'' as amended); '' 50 U.S.C. Ch. 44 (also known as the ''National Security Act of 1947,'' as amended); 50 U.S.C. 3501 *et seq.* (also known as the ''Central Intelligence Agency Act of 1949,'' as amended); Public Law 108–458 (also known as the ''Intelligence Reform and Terrorism Prevention Act of 2004''); and 32 CFR part 2004:

(1) Prescribes industrial security procedures and practices, under E.O. 12829 or successor orders, to safeguard USG classified information that is developed by or disclosed to contractors of the USG.

(2) Prescribes requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information and protect special classes of classified information.

(3) Prescribes that contractors will implement the provisions of this rule no later than 6 months from the effective date of this rule.

§ 117.2 Applicability.

(a) This rule applies to:

(1) The Office of the Secretary of Defense, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (referred to collectively in this rule as the ''DoD Components'').

(2) All executive branch departments and agencies.

(3) All industrial, educational, commercial, or other non-USG entities granted access to classified information by the USG executive branch departments and agencies or by foreign governments.

(4) The release of classified information by the USG to contractors, who are required to safeguard classified information released during all phases of the contracting, agreement (including cooperative research and development agreements), licensing, and grant processes, *i.e.,* the preparation and submission of bids and proposals, negotiation, award, performance, and termination. Also, it applies in situations involving a contract, agreement, license, or grant when actual knowledge of classified information is not required, but reasonable physical security measures cannot be employed to prevent aural or visual access to classified information, because there is the ability and opportunity to gain knowledge of classified information. It also applies to any other situation in which classified information or FGI that is furnished to a contractor requires protection in the interest of national security, but which is not released under a contract, license, certificate or grant.

(b) This rule does not:

(1) Limit in any manner the authority of USG executive branch departments and agencies to grant access to classified information under the cognizance of their department or agency to any individual designated by them. The granting of such access is outside the scope of the NISP and is accomplished pursuant to E.O. 12968, E.O. 13526, E.O. 13691, the AEA, and applicable disclosure policies.

(2) Apply to criminal proceedings in the courts or authorize contractors or their employees to disclose classified information in connection with any criminal proceedings. Defendants and their representative in criminal proceedings in U.S. District Courts, Courts of Appeal, and the U.S. Supreme Court may gain access to classified information in accordance with 18 U.S.C. Appendix 3, Section 1, also known as and referred to in this rule as the ''Classified Information Procedures Act,'' as amended.

§ 117.3 Acronyms and Definitions.

(a) Acronyms. Unless otherwise noted, these acronyms and their terms are for the purposes of this rule.

ACCM alternative compensatory control measures
AEA Atomic Energy Act of 1954, as amended
AUS Australia
CAGE commercial and government entity
CCIPP classified critical infrastructure protection program
CDC cleared defense contractor
CFIUS Committee on Foreign Investment in the United States
CFR Code of Federal Regulations

CI Counterintelligence
CIA Central Intelligence Agency
CNSS Committee on National Security Systems
CNWDI critical nuclear weapons design information
COMSEC communications security
COR central office of record
CSA cognizant security agency
CSO cognizant security office
CUSR Central United States Registry
DCSA Defense Counterintelligence and Security Agency
DD Department of Defense (forms only)
DDTC Directorate of Defense Trade Controls
DGR designated government representative
DHS Department of Homeland Security
DNI Director of National Intelligence
DoD Department of Defense
DoDD Department of Defense Directive
DoDI Department of Defense Instruction
DoDM Department of Defense Manual
DOE Department of Energy
ECP electronic communications plan
E.O. Executive order
FBI Federal Bureau of Investigation
FCL facility (security) clearance
FGI foreign government information
FOCI foreign ownership, control, or influence
FRD Formerly Restricted Data
FSCC Facility Security Clearance Certificate (NATO)
FSO facility security officer
GCA government contracting activity
GCMS government contractor monitoring station
GSA General Services Administration
GSC government security committee
IDE intrusion detection equipment
IDS intrusion detection system
IFB invitation for bid
ISOO Information Security Oversight Office
ISSM information system security manager
ISSO information systems security officer
ITAR International Traffic in Arms Regulations
ITPSO insider threat program senior official
KMP key management personnel
LAA limited access authorization
MFO multiple facility organization
NATO North Atlantic Treaty Organization
NDA nondisclosure agreement
NIAG NATO Industrial Advisory Group
NID national interest determination
NISP National Industrial Security Program
NISPOM National Industrial Security Program Operating Manual
NIST National Institute for Standards and Technology
NNPI Naval Nuclear Propulsion Information
NNSA National Nuclear Security Administration
NPLO NATO Production Logistics Organization
NRC Nuclear Regulatory Commission
NRTL nationally recognized testing laboratory
NSA National Security Agency
NSI national security information
NTIB National Technology and Industrial Base
OCA original classification authority
OMB Office of Management and Budget
PA proxy agreement
PCL personnel (security) clearance
RD Restricted Data
RFP request for proposal
RFQ request for quotation
SAP special access program
SCA security control agreement
SCI sensitive compartmented information
SD Secretary of Defense (forms only)
SEAD Security Executive Agent directive
SF standard form
SMO senior management official
SSA special security agreement
SSP systems security plan
TCP technology control plan
TFNI Transclassified Foreign Nuclear Information
TP transportation plan
UK United Kingdom
UL Underwriters' Laboratories
U.S.C. United States Code
USD (I&S) Under Secretary of Defense for Intelligence and Security
USG United States Government
USML United States Munitions List
VAL visit authorization letter
VT voting trust

(b) Definitions. Unless otherwise noted, these terms and their definitions are for the purposes of this rule.

Access means the ability and opportunity to gain knowledge of classified information.

Access Permittee means the holder of an Access Permit issued pursuant to the regulations set forth in 10 CFR part 725, ''Permits For Access to Restricted Data.''

ACCM are security measures used by USG agencies to safeguard classified intelligence or operations when normal measures are insufficient to achieve strict need-to-know controls and where SAP controls are not required.

Adverse information means any information that adversely reflects on the integrity or character of a cleared employee, that suggests that his or her ability to safeguard classified information may be impaired, that his or her access to classified information clearly may not be in the interest of national security, or that the individual constitutes an insider threat.

Affiliate means each entity that directly or indirectly controls, is directly or indirectly controlled by, or is under common control with, the ultimate parent entity.

Agency(ies) means any ''Executive agency'' as defined in 5 U.S.C. 105; any ''Military department'' as defined in 5 U.S.C. 102; and any other entity within the executive branch that releases classified information to private sector entities. This includes component agencies under another agency or under a cross-agency oversight office (such as ODNI with CIA), which are also agencies for purposes of this rule.

Alarm service company means an entity or branch office from which all of the installation, service, and maintenance of alarm systems are provided, and the monitoring and investigation of such systems are either provided by its own personnel or with personnel assigned by this location.

Alarm system description form means a form describing an alarm system and monitoring information.

Approved security container means a GSA approved security container originally procured through the Federal Supply system. The security containers bear the GSA Approval label on the front face of the container, which identifies them as meeting the testing requirements of the assigned federal specification and having been maintained according to Federal Standard 809.

Approved vault means a vault built to Federal Standard 832 and approved by the CSA.

AUS community consists of the Government of Australia entities and Australian non-governmental facilities identified on the DDTC website (*https://pmddtc.state.gov/*) at the time of export or transfer.

Authorized person means a person who has a favorable determination of eligibility for access to classified information, has signed an approved nondisclosure agreement, and has a need-to-know.

Branch office means an office of an entity which is located somewhere other than the entity's main office location. A branch office is simply another location of the same legal business entity, and is still involved in the business activities of the entity.

CCIPP means security sharing of classified information under a designated critical infrastructure protection program with such authorized individuals and organizations as determined by the Secretary of Homeland Security.

CDC means a subset of contractors cleared under the NISP who have classified contracts with the DoD.

Certification means comprehensive evaluation of an information system component that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

Classification guide means a document issued by an authorized original classifier that identifies the elements of information regarding a specific subject that must be classified and prescribes the level and duration of classification and appropriate declassification instructions.

Classified contract means any contract, license, agreement, or grant requiring access to classified information by a contractor and its

employees for performance. A contract is referred to in this rule as a ''classified contract'' even when the contract document and the contract provisions are not classified. The requirements prescribed for a ''classified contract'' also are applicable to all phases of precontract, license or grant activity, including solicitations (bids, quotations, and proposals), precontract negotiations, post-contract activity, or other government contracting activity (GCA) programs or projects which require access to classified information by a contractor.

Classified covered information system means an information system that is owned or operated by or for a cleared defense contractor and that processes, stores, or transmits information created by or for the DoD with respect to which such contractor is required to apply enhanced protection (*e.g.,* classified information). A classified covered information system is a type of covered network consistent with the requirements of Section 941 of Public Law 112–239 and 10 U.S.C. 391.

Classified information means information that has been determined, pursuant to E.O. 13526, or any predecessor or successor order, and the AEA of 1954, as amended, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The term includes NSI, RD, and FRD.

Classified meetings means a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed.

Classified visit means a visit during which a visitor will require, or is expected to require, access to classified information.

Classifier means any person who makes a classification determination and applies a classification category to information or material. The determination may be an original classification action or it may be a derivative classification action. Contractors make derivative classification determinations based on classified source material, a security classification guide, or a contract security classification specification, or equivalent.

Cleared commercial carrier means a carrier that is authorized by law, regulatory body, or regulation to transport SECRET and CONFIDENTIAL material and has been granted a SECRET facility clearance in accordance with the NISP.

Cleared employees means all employees of industrial or commercial contractors, licensees, certificate holders, or grantees of an agency, as well as all employees of subcontractors and personal services contractor personnel, and who are granted favorable eligibility determinations for access to classified information by a CSA or are being processed for eligibility determinations for access to classified information by a CSA. A contractor may give an employee access to classified information in accordance with the provisions of § 117.10(a)(1)(iii).

Closed area means an area that meets the requirements of this rule for safeguarding classified material that, because of its size, nature, or operational necessity, cannot be adequately protected by the normal safeguards or stored during nonworking hours in approved containers.

CNWDI means a DoD category of TOP SECRET RD or SECRET RD information that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Specifically excluded is information concerning arming, fusing, and firing systems; limited life components; and total contained quantities of fissionable, fusionable, and high explosive materials by type. Among these excluded items are the components that DoD personnel set, maintain, operate, test or replace.

Compromise means an unauthorized disclosure of classified information.

COMSEC means the protective measures taken to deny unauthorized persons information derived from USG telecommunications relating to national security and to ensure the authenticity of such communications.

CONFIDENTIAL means the classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority (OCA) is able to identify or describe.

Consignee means a person, firm, or Government (*i.e.,* USG or foreign government) activity named as the receiver of a shipment; one to whom a shipment is consigned.

Consignor means a person, firm, or Government (*i.e.,* USG or foreign government) activity by which articles are shipped. The consignor is usually the shipper.

Constant surveillance service means a transportation protective service provided by a commercial carrier qualified by the Surface Deployment and Distribution Command to transport CONFIDENTIAL shipments. The service requires constant surveillance of the shipment at all times by a qualified carrier representative; however, an FCL is not required for the carrier. The carrier providing the service must maintain a signature and tally record for the shipment.

Consultant means an individual under contract, and compensated directly, to provide professional or technical assistance to a contractor in a capacity requiring access to classified information.

Continuous evaluation as defined in SEAD 6 is a personnel security investigative process to review the background of a covered individual who has been determined to be eligible for access to classified information or to hold a sensitive position at any time during the period of eligibility. Continuous evaluation leverages a set of automated records checks and business rules, to assist in the ongoing assessment of an individual's continued eligibility. It supplements, but does not replace, the established personnel security program for scheduled periodic reinvestigations of individuals for continuing eligibility.

Continuous monitoring program means a system that facilitates ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions.

Contracting officer means a USG official who, in accordance with departmental or agency procedures, has the authority to enter into and administer contracts, licenses or grants and make determinations and findings with respect thereto, or any part of such authority. The term also includes the designated representative of the contracting officer acting within the limits of his or her authority.

Contractor means any industrial, educational, commercial, or other entity that has been granted an entity eligibility determination by a CSA. This term also includes licensees, grantees, or certificate holders of the USG with an entity eligibility determination granted by a CSA. As used in this rule, ''contractor'' does not refer to contractor employees or other personnel.

Cooperative agreement means a legal instrument which, consistent with 31 U.S.C. 6305, is used to enter into the same kind of relationship as a grant (see definition of ''grant'' in this subpart), except that substantial involvement is expected between USG and the recipient when carrying out the activity contemplated by the cooperative agreement. The term does not include ''cooperative research and development agreements'' as defined in 15 U.S.C. 3710a.

Cooperative research and development agreement means any agreement between one or more Federal laboratories and one or more non-Federal parties under which the Government, through its laboratories, provides personnel, services, facilities, equipment, intellectual property, or other resources with or without reimbursement (but not funds to non-Federal parties) and the non-Federal parties provide funds, personnel, services, facilities, equipment, intellectual property, or other resources toward the conduct of specified research or development efforts which are consistent with the missions of the laboratory; except that such term does not include a procurement contract or cooperative agreement as those terms are used in sections 6303, 6304, and 6305 of title 31.

Corporate family means an entity, its parents, subsidiaries, divisions, and branch offices.

Counterintelligence means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs.

Courier means a cleared employee, designated by the contractor, whose principal duty is to transmit classified material to its destination, ensuring that the classified material remains under their constant and continuous protection and that they make direct point-to-point delivery.

CRYPTO means the marking or designator that identifies unencrypted COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive USG or USG-derived information. This includes non-split keying material used to encrypt or decrypt COMSEC critical software and software based algorithms.

CSA means an agency designated as having NISP implementation and security responsibilities for its own agencies (including component agencies) and any entities and non-CSA agencies under its cognizance. The CSAs are: DoD; DOE; NRC; ODNI; and DHS.

CSO means an organizational unit to which the head of a CSA delegates authority to administer industrial security services on behalf of the CSA.

CUI means information the USG creates or possesses, or that an entity creates or possesses for or on behalf of the USG, that a law, regulation, or USG-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency.

Custodian means an individual who has possession of, or is otherwise charged with, the responsibility for safeguarding classified information.

Cybersecurity means prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Cyber incident means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Declassification means a date or event which coincides with the lapse of the information's national security sensitivity, as determined by the OCA. Declassification occurs when the OCA has determined that the classified information no longer requires, in the interest of national security, any degree of protection against unauthorized disclosure, and the information has had its classification designation removed or cancelled.

Defense articles means those articles, services, and related technical data, including software, in tangible or intangible form, which are listed on the United States Munitions List (USML) of the International Traffic in Arms Regulations (ITAR), as modified or amended. Defense articles exempt from the scope of ITAR section 126.17 are identified in Supplement No. 1 to Part 126 of the ITAR.

Defense services means:

(1) Furnishing assistance (including training) to foreign persons, whether in the United States or abroad, in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles;

(2) Furnishing to foreign persons any controlled technical data, whether in the United States or abroad; or

(3) Providing military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

Derivative classification means the incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes classifying information based on classification guidance. Duplicating or reproducing existing classified information is not derivative classification.

Document means any recorded information, regardless of the nature of the medium, or the method or circumstances of recording.

Downgrade means a determination by a declassification authority that information classified and safeguarded at a specified level will be classified and safeguarded at a lower level.

Embedded system means an information system that performs or controls a function, either in whole or in part, as an integral element of a larger system or subsystem, such as, ground support equipment, flight simulators, engine test stands, or fire control systems.

Empowered official is defined in 22 CFR part 120.

Entity is a generic and comprehensive term which may include sole proprietorships, partnerships, corporations, limited liability companies, societies, associations, institutions, contractors, licensees, grantees, certificate holders, and other organizations usually established and operating to carry out a commercial, industrial, educational, or other legitimate business, enterprise, or undertaking, or parts of these organizations. It may reference an entire organization, a prime contractor, parent organization, a branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity (referred to as ''sub-entities'' when necessary to distinguish such entities from prime or parent entities). It may also reference a specific location or facility, or the headquarters or official business location of the organization, depending upon the organization's business structure, the access needs involved, and the responsible CSA's procedures. The term ''entity'' as used in this rule refers to the particular entity to which an agency might release, or is releasing, classified information, whether that entity is a parent or

subordinate organization. The term ''entity'' in this rule includes contractors.

Entity eligibility determination means an assessment by the CSA as to whether an entity is eligible for access to classified information of a certain level (and all lower levels). Entity eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable entity eligibility determination results in eligibility to access classified information under the cognizance of the responsible CSA to the level approved. When the entity would be accessing categories of information such as RD or SCI for which the CSA for that information has set additional requirements, CSAs must also assess whether the entity is eligible for access to that category of information. Some CSAs refer to their favorable entity eligibility determinations as FCLs. However, a favorable entity eligibility determination for the DHS CCIPP is not equivalent to an FCL and does not meet the requirements for FCL reciprocity. A favorable entity eligibility determination does not convey authority to store classified information.

Escort means a cleared person, designated by the contractor, who accompanies a shipment of classified material to its destination. The classified material does not remain in the personal possession of the escort but the conveyance in which the material is transported remains under the constant observation and control of the escort.

Extent of protection means the designation (such as ''Complete'') used to describe the degree of alarm protection installed in an alarmed area.

Facility means a plant, laboratory, office, college, university, or commercial structure with associated warehouses, storage areas, utilities, and components, that, when related by function and location, form an operating entity.

FCL means an administrative determination that, from a security viewpoint, an entity is eligible for access to classified information of a certain level (and all lower levels) (*e.g.,* a type of favorable entity eligibility determination used by some CSAs). An entity eligibility determination for the DHS CCIPP is not the equivalent of an FCL and does not meet the requirements for FCL reciprocity.

FGI means information that is:

(1) Provided to the United States by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, expressed or implied, that the information, the source of the information, or both, are to be held in confidence; or

(2) Produced by the United States pursuant to, or as a result of, a joint arrangement with a foreign government or governments, an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both are to be held in confidence.

Foreign interest means any foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States.

Foreign national means any person who is not a citizen or national of the United States.

Foreign person is defined in 31 CFR 800.224 for CFIUS purposes.

FRD means classified information removed from the Restricted Data category upon a joint determination by the DOE and DoD that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information.

Freight forwarder (transportation agent) means any agent or facility designated to receive, process, and transship U.S. material to foreign recipients. In the context of this rule, it means an agent or facility cleared specifically to perform these functions for the transfer of U.S. classified material to foreign recipients.

GCA means an element of an agency that the agency head has designated and delegated broad authority regarding acquisition functions. A foreign government may also be a GCA.

Governing board means an entity's board of directors, board of managers, board of trustees, or equivalent governing body.

Grant means a legal instrument which, consistent with 31 U.S.C. 6304, is used to enter into a relationship: (a) Of which the principal purpose is to transfer a thing of value to the recipient to carry out a public purpose of support or stimulation authorized by a law of the United States, rather than to acquire property or services for the USG's direct benefit or use; or, (b) In which substantial involvement is not expected between DoD and the recipient when carrying out the activity contemplated by the award. Throughout this rule, the term grant will include both the grant and cooperative agreement.

Grantee means the entity that receives a grant or cooperative agreement.

Hand carrier means a cleared employee, designated by the contractor, who occasionally hand carries classified material to its destination in connection with a classified visit or meeting. The classified material remains in the personal possession of the hand carrier except for authorized overnight storage.

Home office means the headquarters of a multiple facility entity.

Industrial security means that portion of information security concerned with the protection of classified information in the custody of U.S. industry.

Information means any knowledge that can be communicated or documentary material, regardless of its physical form or characteristics.

Information security means the system of policies, procedures, and requirements established pursuant to executive order, statute, or regulation to protect information that, if subjected to unauthorized disclosure, could reasonably be expected to cause damage to national security. The term also applies to policies, procedures, and requirements established to protect unclassified information that may be withheld from release to the public.

Information system means an assembly of computer hardware, software, and firmware configured for the purpose of automating the functions of calculating, computing, sequencing, storing, retrieving, displaying, communicating, or otherwise manipulating data, information and textual material.

Insider means cleared contractor personnel with authorized access to any USG or contractor resource, including personnel, facilities, information, equipment, networks, and systems.

Insider threat means the likelihood, risk, or potential that an insider will use his or her authorized access, wittingly or unwittingly, to do harm to the national security of the United States. Insider threats may include harm to contractor or program information, to the extent that the information impacts the contractor or agency's obligations to protect classified NSI.

Joint venture means an association of two or more persons or entities engaged in a single defined project with all parties contributing assets and efforts, and sharing in the management, profits and losses, in accordance with the terms of an agreement among the parties.

KMP means an entity's senior management official (SMO), facility security officer (FSO), insider threat program senior official (ITPSO), and all other entity officials who either hold majority interest or stock in, or have

direct or indirect authority to influence or decide issues affecting the management or operations of, the entity or classified contract performance.

L access authorization means an access determination that is granted by DOE or NRC based on a Tier 3 or successor background investigation as set forth in applicable national-level requirements and DOE directives. Within DOE and NRC, an ''L'' access authorization permits an individual who has an official ''need to know'' to access Confidential Restricted Data, Secret and Confidential Formerly Restricted Data, Secret and Confidential Transclassified Foreign Nuclear Information, or Secret and Confidential National Security Information, required in the performance of official duties. An ''L'' access authorization determination is required for individuals with a need to know outside of DOE, NRC, DoD, and in limited cases NASA, to access Confidential Restricted Data.

LAA means security access authorization to CONFIDENTIAL or SECRET information granted to non-U.S. citizens requiring only limited access in the course of their regular duties.

Material means any product or substance on or in which information is embodied.

Matter means anything in physical form that contains or reveals classified information.

Media means physical devices or writing surfaces including but not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

MFO means a legal entity (single proprietorship, partnership, association, trust, or corporation) composed of two or more entities (facilities).

National of the United States means a person who owes permanent allegiance to the United States. All U.S. citizens are U.S. nationals; however, not all U.S. nationals are U.S. citizens (for example, persons born in American Samoa or Swains Island).

NATO information means information bearing NATO markings, indicating the information is the property of NATO, access to which is limited to representatives of NATO and its member nations unless NATO authority has been obtained to release outside of NATO.

NATO visits means visits by personnel representing a NATO entity and relating to NATO contracts and programs.

Need-to-know means a determination made by an authorized holder of classified information that a prospective recipient has a requirement for access to, knowledge of, or possession of the classified information to perform tasks or services essential to the fulfillment of a classified contract or program.

Network means a system of two or more information systems that can exchange data or information.

NNPI is classified or unclassified information concerning the design, arrangement, development, manufacture, testing, operation, administration, training, maintenance, and repair of the propulsion plants of naval nuclear-powered ships and prototypes, including the associated shipboard and shore-based nuclear support facilities.

Non-DoD executive branch agencies means the non-DoD agencies that have entered into agreements with DoD to receive NISP industrial security services from DoD. A list of these agencies is on the Defense Counterintelligence and Security Agency website at *https://www.dcsa.mil.*

Non-Federal information system is defined in 32 CFR part 2002.

NRTL means a private sector organizations recognized by the Occupational Safety and Health Administration to perform certification for certain products to ensure that they meet the requirements of both the construction and general industry Occupational Safety and Health Administration electrical standards. Each NRTL is recognized for a specific scope of test standards.

NSI means information that has been determined pursuant to E.O. 13526 or predecessor order to require protection against unauthorized disclosure and marked to indicate its classified status.

NTIB means the industrial bases of the United States and Australia, Canada, and the United Kingdom.

NTIB entity means a person that is a subsidiary located in the United States for which the ultimate parent entity and any intermediate parent entities of such subsidiary are located in a country that is part of the national technology and industrial base (as defined in section 2500 of title 10, United States Code); and that is subject to the foreign ownership, control, or influence requirements of the National Industrial Security Program.

Nuclear weapon data means Restricted Data or Formerly Restricted Data concerning the design, manufacture, or utilization (including theory, development, storage, characteristics, performance and effects) of nuclear explosives, nuclear weapons or nuclear weapon components, including information incorporated in or related to nuclear explosive devices. Nuclear weapon data is matter in any combination of documents or material, regardless of physical form or characteristics.

OCA means an individual authorized in writing, either by the President, the Vice President, or by agency heads or other officials designated by the President, to classify information in the first instance.

Original classification means an initial determination that information requires, in the interest of national security, protection against unauthorized disclosure. Only USG officials who have been designated in writing may apply an original classification to information.

Parent means an entity that owns at least a majority of another entity's voting securities.

PCL means an administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted.

Prime contract means a contract awarded by a GCA to a contractor for a legitimate USG purpose.

Prime contractor means the contractor who receives a prime contract from a GCA.

Privileged user means a user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Proscribed information means:

(1) TOP SECRET information;

(2) COMSEC information or material, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys.

(3) RD;

(4) SAP information; or.

(5) SCI.

Protective security service means a transportation protective service provided by a cleared commercial carrier qualified by DoD's Surface Deployment and Distribution Command to transport SECRET shipments.

Q access authorization means an access determination that is granted by DOE or NRC based on a Tier 5 or successor background investigation as set forth in applicable national-level requirements and DOE directives. Within DOE and the NRC, a ''Q'' access authorization permits an individual with an official ''need to know'' to access Top Secret, Secret and Confidential Restricted Data, Formerly Restricted Data, Transclassified Foreign

Nuclear Information, National Security Information, or special nuclear material in Category I or II quantities, as required in the performance of official duties. A ''Q'' access authorization is required for individuals with a need to know outside of DOE, NRC, DoD, and in a limited case NASA, to access Top Secret and Secret Restricted Data.

Remote terminal means a device communicating with an automated information system from a location that is not within the central computer facility.

Restricted area means a controlled access area established to safeguard classified material that, because of its size or nature, cannot be adequately protected during working hours by the usual safeguards, but is capable of being stored during non-working hours in an approved repository or secured by other methods approved by the CSA.

RD means all data concerning (1) design, manufacture, or utilization of atomic weapons; (2) the production of special nuclear material; or (3) the use of special nuclear material in the production of energy, but does not include data declassified or removed from the RD category pursuant to section 142 of the AEA.

SAP means any program that is established to control access and distribution and to provide protection for particularly sensitive classified information beyond that normally required for TOP SECRET, SECRET, or CONFIDENTIAL information. A SAP can be created or continued only as authorized by a senior agency official delegated such authority pursuant to E.O. 13526.

Schedule 13D means a form required by the Securities and Exchange Commission when a person or group of persons acquires beneficial ownership of more than 5% of a voting class of a company's equity securities registered under Section 12 of the ''Securities Exchange Act of 1934'' (available at: *https://www.sec.gov/fast-answers/answerssched13htm.html*).

SCI means a subset of classified national intelligence concerning or derived from intelligence sources, methods or analytical processes that is required to be protected within formal access control systems established by the DNI.

SECRET means the classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the OCA is able to identify or describe.

Security in depth means a determination made by the CSA that a contractor's security program consists of layered and complementary security controls sufficient to deter and detect unauthorized entry and movement within the facility. Examples include, but are not limited to, use of perimeter fences, employee and visitor access controls, use of an Intrusion Detection System (IDS), random guard patrols throughout the facility during nonworking hours, closed circuit video monitoring, or other safeguards that mitigate the vulnerability of open storage areas without alarms and security storage cabinets during nonworking hours.

Security violation means failure to comply with the policy and procedures established by this part that reasonably could result in the loss or compromise of classified information.

Shipper means one who releases custody of material to a carrier for transportation to a consignee. (See also ''Consignor.'')

SMO is the contractor's official responsible for the entity policy and strategy. The SMO is an entity employee occupying a position in the entity with ultimate authority over the facility's operations and the authority to direct actions necessary for the safeguarding of classified information in the facility. This includes the authority to direct actions necessary to safeguard classified information when the access to classified information by the facility's employees is solely at other contractor facilities or USG locations.

Source document means an existing document that contains classified information that is incorporated, paraphrased, restated, or generated in new form into a new document.

Standard practice procedures means a document prepared by a contractor that implements the applicable requirements of this rule for the contractor's operations and involvement with classified information at the contractor's facility.

Subcontract means any contract entered into by a contractor to furnish supplies or services for performance of a prime contract or a subcontract. It includes a contract, subcontract, purchase order, lease agreement, service agreement, request for quotation (RFQ), request for proposal (RFP), invitation for bid (IFB), or other agreement or procurement action between contractors that requires or will require access to classified information to fulfill the performance requirements of a prime contract.

Subcontractor means a supplier, distributor, vendor, or firm that enters into a contract with a prime contractor to furnish supplies or services to or for the prime contractor or another subcontractor. For the purposes of this rule, each subcontractor will be considered as a prime contractor in relation to its subcontractors.

Subsidiary means an entity in which another entity owns at least a majority of its voting securities.

System software means computer programs that control, monitor, or facilitate use of the information system; for example, operating systems, programming languages, communication, input-output controls, sorts, security packages, and other utility-type programs. Also includes off-the-shelf application packages obtained from manufacturers and commercial vendors, such as for word processing, spreadsheets, data base management, graphics, and computer-aided design.

Technical data means:

(1) Information, other than software, which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions or documentation.

(2) Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List.

(3) Information covered by an invention secrecy order.

(4) Software directly related to defense articles.

TFNI means classified information concerning the nuclear energy programs of other nations (including subnational entities) removed from the RD category under section 142(e) of the AEA after the DOE and the Director of National Intelligence jointly determine that it is necessary to carry out intelligence-related activities under the provisions of the National Security Act of 1947, as amended, and that it can be adequately safeguarded as NSI instead. This includes information removed from the RD category by past joint determinations between DOE and the CIA. TFNI does not include information transferred to the United States under an Agreement for Cooperation under the Atomic Energy Act or any other agreement or treaty in which the United States agrees to protect classified information.

TOP SECRET means the classification level applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the OCA is able to identify or describe.

Transmission means sending information from one place to another by radio, microwave, laser, or other non-connective methods, as well as by cable, wire, or other connective medium. Transmission also includes movement involving the actual transfer of custody and responsibility for a document or other classified material from one authorized addressee to another.

Transshipping activity means a government activity to which a carrier transfers custody of freight for reshipment by another carrier to the consignee.

UK community consists of the UK Government entities with facilities and UK non-governmental facilities identified on the DDTC website (*https://www.pmddtc.state.gov/*) at the time of export.

Unauthorized person means a person not authorized to have access to specific classified information in accordance with the requirements of this rule.

United States means the 50 states and the District of Columbia.

United States and its territorial areas means the 50 states, the District of Columbia, Puerto Rico, Guam, American Samoa, the Virgin Islands, Wake Island, Johnston Atoll, Kingman Reef, Palmyra Atoll, Baker Island, Howland Island, Jarvis Island, Midway Islands, Navassa Island, and Northern Mariana Islands.

Upgrade means a determination that certain classified information, in the interest of national security, requires a higher degree of protection against unauthorized disclosure than currently provided, coupled with a change to the classification designation to reflect the higher degree.

U.S. classified cryptographic information means a cryptographic key and authenticators that are classified and are designated as TOP SECRET CRYPTO or SECRET CRYPTO. This means all cryptographic media that embody, describe, or implement classified cryptographic logic, to include, but not limited to, full maintenance manuals, cryptographic descriptions, drawings of cryptographic logic, specifications describing a cryptographic logic, and cryptographic software, firmware, or repositories of such software such as magnetic media or optical disks.

U.S. person means a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments.

Voting securities means any securities that presently entitle the owner or holder thereof to vote for the election of directors of the issuer or, with respect to unincorporated entities, individuals exercising similar functions.

Working hours means the period of time when:

(1) There is present in the specific area where classified material is located, a work force on a regularly scheduled shift, as contrasted with employees working within an area on an overtime basis outside of the scheduled work shift; and

(2) The number of employees in the scheduled work force is sufficient in number and so positioned to be able to detect and challenge the presence of unauthorized personnel. This would, therefore, exclude janitors, maintenance personnel, and other individuals whose duties require movement throughout the facility.

Working papers means documents or materials, regardless of the media, which are expected to be revised prior to the preparation of a finished product for dissemination or retention.

§ 117.4 Policy.

E.O. 12829 established the NISP to serve as a single, integrated, cohesive industrial security program to protect classified information and preserve our Nation's economic and technological interests.

(a) When contracts, licenses, agreements, and grants to contractors require access to classified information, national security requires that this information be safeguarded in a manner equivalent to its protection within the executive branch of the USG.

(b) National security requires that the industrial security program promote the economic and technological interests of the United States. Redundant, overlapping, or unnecessary requirements impede those interests.

§ 117.5 Information collections.

The information collection requirements are:

(a) *Standard Form (SF) 328* ''Certificate Pertaining to Foreign Interest'' (available at: *https://www.gsa.gov/forms-library/certificate-pertaining-foreign-interests*) in § 117.8 and § 117.11, is assigned Office of Management and Budget (OMB) Control Number 0704–0579. The expiration date of this information collection is listed in the DoD Information Collections System at *https://apps.sp.pentagon.mil/sites/dodiic/Pages/default.aspx.*

(b) *NRC collection.* ''Facility Security Clearance and Safeguarding of National Security Information and Restricted Data,'' is assigned OMB Control Number: 3150–0047. Under this collection, NRC-regulated facilities and other organizations are required to provide information and maintain records to ensure that an adequate level of protection is provided to NRC-classified information and material.

(c) *DOE collection.* ''Security,'' a NISP CSA information collection, is assigned OMB Control Number: 1910–1800. This information collection, which includes facility security clearance information, is used by the DOE to exercise management, oversight, and control over its contractors' management and operation of DOE's Government-owned contractor-operated facilities, and over its offsite contractors. The contractor management, oversight, and control functions relate to the ways in which DOE contractors provide goods and services for DOE organizations and activities in accordance with the terms of their contracts and the applicable statutory, regulatory, and mission support requirements of the Department. Information collected from private industry and private individuals is used to protect national security and critical assets entrusted to the Department.

(d) *DoD collection.* ''DoD Security Agreement,'' is assigned OMB Control Number: 0704–0194. ''National Industrial Security System,'' a CSA information collection, is assigned OMB Control Number: 0704–0571, and is a DoD information collection used to conduct its monitoring and oversight of contractors. Department of Defense ''Contract Security Classification Specification,'' (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/dd/dd0254.pdf* and available at: *https://www.dcsa.mil/is/nccs/*), is assigned OMB Control Number 0704–0567 and used by both DoD and agencies which have an industrial security agreement with DoD. ''Defense Information System for Security,'' is assigned OMB Control Number: 0704–0573. Defense Information System for Security is a DoD automated system for personnel security, providing a common, comprehensive medium to record, document, and identify personal security actions within DoD including submitting adverse information, verification of security clearance status, requesting investigations, and supporting continuous evaluation activities. It requires personal data collection to facilitate the initiation, investigation and adjudication of information relevant to DoD security clearances and employment suitability

determinations for active duty military, civilian employees and contractors seeking such credentials. Joint Personnel Adjudicative System is assigned OMB Control Number: 0704–0496. Joint Personnel Adjudicative System is an information system which requires personal data collection to facilitate the initiation, investigation and adjudication of information relevant to DoD security clearances and employment suitability determinations for active duty military, civilian employees and contractors seeking such credentials.

§ 117.6 Responsibilities.

(a) *Under Secretary of Defense for Intelligence & Security (USD(I&S)).* The USD(I&S), on behalf of the Secretary of Defense, and in accordance with E.O. 12829, 32 CFR part 2004, and DoDI 5220.22:

(1) Carries out the direction in section 201 of E.O. 12829 that the Secretary of Defense issue and maintain this rule and changes to it. The USD(I&S) does so in consultation with all affected agencies (E.O. 12829 section 201), with the concurrence of the Secretary of Energy, the Chairman of the NRC, the DNI, and the Secretary of Homeland Security (E.O.12829 section 201), and in consultation with the ISOO Director (E.O. 12829 section 102).

(2) Acts as the CSA for DoD.

(3) Provides policy and management of the NISP for non-DoD executive branch agencies who enter into inter-agency security agreements with DoD to provide industrial security services required when classified information is disclosed to contractors in accordance with E.O. 12829, as amended.

(b) *Director, DCSA.* Under the authority, direction, and control of the USD(I&S), and in accordance with DoDI 5220.22 and DoD Directive (DoDD) 5105.42, ''Defense Security Service (DSS)'' [1] (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/510542p.pdf?ver=2019-01-14-090012-283*) the Director, DCSA:

(1) Oversees and manages DCSA, which serves as the DoD CSO.

(2) Administers the NISP as a separate program element on behalf of DoD GCAs and those agencies with agreements with DoD for security services.

(3) Provides security oversight of the NISP as the DoD CSO on behalf of DoD components and those non-DoD executive branch agencies who enter into agreements with DoD as noted in paragraph (a)(3) of this section. The Director, DCSA, will be relieved of this oversight function for DoD special access programs (SAPs) when the Secretary of Defense or the Deputy Secretary of Defense approves a carve-out provision in accordance with DoDD 5205.07, ''DoD SAP Policy'' (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/520507p.pdf?ver=2020-02-04-142942-827*).

(c) *Secretary of Energy.* In addition to the responsibilities in paragraph (h) of this section, the Secretary of Energy:

(1) Prescribes procedures for the portions of this rule pertaining to information classified under the AEA (*i.e.,* RD, FRD, and TFNI), as nothing in the rule shall be construed to supersede the authority of the Secretary of Energy under the AEA.

(2) Retains authority over access to information classified under the AEA.

(3) Inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to information classified under the AEA, as necessary.

(d) *Chairman of the NRC.* In addition to the responsibilities in paragraph (h) of this section, the Chairman of the NRC:

(1) Prescribes procedures for the portions of this rule that pertain to information under NRC programs classified under the AEA, other federal statutes, and executive orders.

(2) Retains authority over access to information under NRC programs classified under the AEA, other federal statutes, and executive orders.

(3) Inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to information under NRC programs classified pursuant to the AEA, other federal statutes, and executive orders where appropriate.

(e) *DNI.* In addition to the responsibilities in paragraph (h) of this section, the DNI:

(1) Prescribes procedures for the portions of this rule pertaining to intelligence sources, methods, and activities, including, but not limited to, SCI.

(2) Retains authority over access to intelligence sources, methods, and activities, including SCI.

(3) Provides guidance on the security requirements for intelligence sources and methods of information, including, but not limited to, SCI.

(f) *Secretary of Homeland Security.* In accordance with E.O. 12829, E.O. 13691, and in addition to the responsibilities in paragraph (h) of this section, the Secretary of Homeland Security:

(1) Prescribes procedures for the portions of this rule that pertain to the CCIPP.

(2) Retains authority over access to information under the CCIPP.

(3) Inspects and monitors contractor, licensee, certificate holder, and grantee programs and facilities that involve access to CCIPP.

(g) *All the CSA heads.* The CSA heads:

(1) Oversee the security of classified contracts and activities under their purview.

(2) Provide oversight of contractors under their security cognizance.

(3) Minimize redundant and duplicative security review and audit activities of contractors, including such activities conducted at contractor locations where multiple CSAs have equities.

(4) Execute appropriate intra-agency and inter-agency agreements to avoid redundant and duplicate reviews.

(5) Designate one or more CSOs for security administration.

(6) Designate subordinate officials, in accordance with governing policies, to act as the authorizing official. Authorizing officials will:

(i) Assess and authorize contractors to process classified information on information systems.

(ii) Conduct oversight of such information system processing and provide information system security guidelines in accordance with Federal information system security control policies, standards, and procedures. Minimize redundant and duplicative security review and audit activity of contractors, including such activity conducted at contractor locations where multiple CSAs have equities.

(h) *Heads of component agencies.* In accordance with applicable CSA direction, the component agency heads:

(1) Oversee compliance with procedures identified by the applicable CSA or designated CSO.

(2) Provide oversight of contractor personnel visiting or working on USG installations.

(3) Promptly apprise the CSO of information received or developed that could adversely affect a cleared contractor, licensee, or grantee, and their employees, to hold an FCL or PCL, or that otherwise raises substantive doubt about their ability to safeguard classified information entrusted to them.

(4) Propose changes to this rule as deemed appropriate and provide them

[1] On June 20, 2020, the Secretary of Defense renamed the Defense Security Service (DSS) as the Defense Counterintelligence and Security Agency (DCSA), as required by Executive Oder 13467, section 2.6(b)(i) (as amended by Executive Order 13968, Apr. 24, 2019, 84 FR 18125). Pursuant to Section 4 of E.O. 13968, references to DSS in DoD issuances should be deemed or construed to refer to DCSA.

to the applicable CSA for submission to the OUSD(I&S) Counterintelligence, Law Enforcement and Security Directorate.

(i) *Director, ISOO.* The Director, ISOO:

(1) Oversees the NSIP and agency compliance with it, in accordance with E.O. 12829.

(2) Issues and maintains the NISP implementing directive (32 CFR part 2004), in accordance with E.O. 12829, to provide guidance to the CSAs and USG agencies under the NISP.

(3) Chairs the NISP Policy Advisory Committee. Addresses complaints and suggestions from contractors, as detailed in the NISP Policy Advisory Committee bylaws.

§ 117.7 Procedures.

(a) *General.* Contractors will protect all classified information that they are provided access to or that they possess. This responsibility applies at both contractor and USG locations.

(b) *Contractor Security Officials.* Contractors will appoint security officials who are U.S. citizens, except in exceptional circumstances (see § 117.9(m) and § 117.11(e)).

(1) Appointed security officials listed in paragraphs (b)(2), (b)(3), and (b)(4) of this section must:

(i) Oversee the implementation of the requirements of this rule. Depending upon the size and complexity of the contractor's security operations, a single contractor employee may serve in more than one position.

(ii) Undergo the same security training that is required for all other contractor employees pursuant to § 117.12, in addition to their position specific training.

(iii) Be designated in writing with their designation documented in accordance with CSA guidance.

(iv) Undergo a personnel security investigation and national security eligibility determination for access to classified information at the level of the entity's eligibility determination for access to classified information (*e.g.,* FCL level) and be on the KMP list for the cleared entity.

(2) *SMO.* The SMO will:

(i) Ensure the contractor maintains a system of security controls in accordance with the requirements of this rule.

(ii) Appoint a contractor employee or employees, in writing, as the FSO and appoint the same employee or a different employee as the ITPSO. The SMO may appoint a single employee for both roles or may appoint one employee as the FSO and a different employee as the ITPSO.

(iii) Remain fully informed of the facility's classified operations.

(iv) Make decisions based on classified threat reporting and their thorough knowledge, understanding, and appreciation of the threat information and the potential impacts caused by a loss of classified information.

(v) Retain accountability for the management and operations of the facility without delegating that accountability to a subordinate manager.

(3) *FSO.* The FSO will:

(i) Supervise and direct security measures necessary for implementing the applicable requirements of this rule and the related USG security requirements to ensure the protection of classified information.

(ii) Complete security training pursuant to § 117.12 and as deemed appropriate by the CSA.

(4) *ITPSO.* The ITPSO will establish and execute an insider threat program.

(i) If the appointed ITPSO is not also the FSO, the ITPSO will ensure that the FSO is an integral member of the contractor's insider threat program.

(ii) The ITPSO will complete training pursuant to § 117.12.

(iii) An entity family may choose to establish an entity family-wide insider threat program with one senior official appointed, in writing, to establish, and execute the program as the ITPSO. Each cleared entity using the entity-wide ITPSO must separately appoint that person as its ITPSO for that facility. The ITPSO will provide an implementation plan to the CSA for executing the insider threat program across the entity family.

(5) *ISSM.* Contractors who are, or will be, processing classified information on an information system located at the contractor facility will appoint an employee to serve as the ISSM. The ISSM must be eligible for access to classified information to the highest level of the information processed on the system(s) under their responsibility. The contractor will ensure that the ISSM is adequately trained and possesses technical competence commensurate with the complexity of the contractor's classified information system. The contractor will notify the applicable CSA if there is a change in the ISSM. The ISSM will oversee development, implementation, and evaluation of the contractor's classified information system program. ISSM responsibilities are in § 117.18.

(6) *Employees performing security duties.* Those employees whose official duties include performance of NISP-related security functions will complete security training tailored to the security functions performed. This training requirement also applies to consultants whose official duties include security functions.

(c) *Other KMP.* In addition to the SMO, the FSO, and the ITPSO, the contractor will include on the KMP list, subject to CSA concurrence, any other officials who either hold majority interest or stock in the entity, or who have direct or indirect authority to influence or decide issues affecting the management or operations of the contractor or issues affecting classified contract performance. The CSA may either:

(1) Require these KMP to be determined to be eligible for access to classified information as a requirement for the entity's eligibility determination or;

(2) Allow the entity to formally exclude these KMP from access to classified information. The entity's governing board will affirm the exclusion by issuing a formal action (see table), and provide a copy of the exclusion action to the CSA. The entity's governing board will document this exclusion action.

TABLE 1 TO PARAGRAPH (c)(2)—EXCLUSION RESOLUTIONS

Type of affirmation	Language to be used in exclusion action
Affirmation for Exclusion from Access to Classified Information.	[Insert name and address of entity or name and position of officer, director, partner, or similar entity official or officials] will not require, will not have, and can be effectively and formally excluded from, access to all classified information disclosed to the entity and does not occupy a position that would enable them to adversely affect the organization's policies or practices in the performance of classified contracts.

TABLE 1 TO PARAGRAPH (c)(2)—EXCLUSION RESOLUTIONS—Continued

Type of affirmation	Language to be used in exclusion action
Affirmation for Exclusion from Higher-level Classified Information.	[Insert name and address of entity or name and position of officer, director, partner, or similar entity official or officials] will not require, will not have, and can be effectively and formally excluded from access to [insert SECRET or TOP SECRET] classified information and does not occupy a position that would enable them to adversely affect the organization's policies or practices in the performance of [insert SECRET or TOP SECRET] classified contracts.

(d) *Insider Threat Program.* Pursuant to this rule and CSA provided guidance to supplement unique CSA mission requirements, the contractor will establish and maintain an insider threat program to gather, integrate, and report relevant and available information indicative of a potential or actual insider threat, consistent with E.O. 13587 and Presidential Memorandum ''National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs.''

(e) *Standard practice procedures.* The contractor will implement all applicable provisions of this rule at each of its cleared facility locations. The contractor will prepare written procedures when the CSA determines them to be necessary to reasonably exclude the possibility of loss or compromise of classified information, and in accordance with additional CSA-provided guidance, as applicable.

(f) *Cooperation with Federal agencies.* Contractors will cooperate with Federal agencies and their officially credentialed USG or contractor representatives during official reviews, investigations concerning the protection of classified information, or personnel security investigations of present or former employees and others (*e.g.,* consultants or visitors). At a minimum, cooperation includes:

(1) Providing suitable arrangements within the facility for conducting private interviews with employees during normal working hours;

(2) Providing, when requested, relevant employment or personnel files, security records, supervisory files, records pertinent to insider threat (*e.g.,* security, cybersecurity, and human resources) and any other records pertaining to an individual under investigation that are, in the possession or control of the contractor or the contractor's representatives or located in the contractor's offices;

(3) Providing access to employment and security records that are located at an offsite location; and

(4) Rendering other necessary assistance.

(g) *Security training and briefings.* Contractors will advise all cleared employees, including those assigned to USG locations or operations outside the United States, of their individual responsibility for classification management and for safeguarding classified information. Contractors will provide security training to cleared employees consisting of initial briefings, refresher briefings, and debriefings in accordance with § 117.12.

(h) *Security reviews*—(1) *USG reviews.* The applicable CSA will conduct recurring oversight reviews of contractors' NISP security programs to verify that the contractor is protecting classified information and implementing the provisions of this rule. The contractor's participation in the security review is required for maintaining the entity's eligibility for access to classified information.

(i) *Review cycle.* The CSA will determine the scope and frequency of security reviews, which may be increased or decreased consistent with risk management principles.

(ii) *Procedures.* (A) The CSA will generally provide notice to the contractor of a forthcoming review, but may also conduct unannounced reviews at its discretion. The CSA security review may subject contractor employees and all areas and receptacles under the control of the contractor to examination.

(B) The CSA will make every effort to avoid unnecessary intrusion into the personal effects of contractor personnel.

(C) The CSA may conduct physical examinations of the interior space of containers not authorized to secure classified material. Such examinations will always be accomplished in the presence of a representative of the contractor.

(iii) *Controlled unclassified information (CUI).* 32 CFR part 2002 requires agencies to implement CUI requirements, but compliance with CUI requirements is outside the scope of the NISP and this rule. However, CSAs may conduct CUI assessments in conjunction with NISP USG reviews when:

(A) The contractor is a participant in the NISP based on a requirement to access classified information;

(B) A classified contract under the CSA's cognizance includes provisions for access to, or protection or handling of, CUI; and

(C) The CSA has provided the contractor with specific guidance regarding the assessment criteria and methodology it will use for overseeing protection of the CUI being accessed, stored or transmitted by the contractor as part of the classified contract.

(2) *Contractor reviews.* Contractors will review their security programs on a continuing basis and conduct a formal self-inspection at least annually and at intervals consistent with risk management principles.

(i) Self-inspections will include the review of the classified activity, classified information, classified information systems, conditions of the overall security program, and the insider threat program. They will have sufficient scope, depth, and frequency, and will have management support during the self-inspection and during remedial actions taken as a result of the self-inspection. Self-inspections will include the review of samples representing the contractor's derivative classification actions, as applicable.

(ii) The contractor will prepare a formal report describing the self-inspection, its findings, and its resolution of issues discovered during the self-inspection. The contractor will retain the formal report for CSA review until after the next CSA security review is completed.

(iii) The SMO at the cleared facility will annually certify to the CSA, in writing, that a self-inspection has been conducted, that other KMP have been briefed on the results of the self-inspection, that appropriate corrective actions have been taken, and that management fully supports the security program at the cleared facility in the manner as described in the certification.

(i) *Contractors working at USG locations.* Contractor employees performing work within the confines of a USG facility will safeguard classified information according to the procedures of the host installation or agency.

(j) *Hotlines.* Federal agencies maintain hotlines to provide an unconstrained avenue for USG and contractor employees to report, without fear of reprisal, known or suspected instances

of security irregularities and infractions concerning contracts, programs, or projects. These hotlines do not supplant the contractor's responsibility to facilitate reporting and timely investigations of security issues concerning its operations or personnel. Contractor personnel are encouraged to report information through established contractor channels. The hotline may be used as an alternate means to report this type of information. Contractors will inform all personnel that hotlines may be used for reporting issues of national security significance. Each CSA will post hotline information and telephone numbers on their websites for contractor access.

(k) *Agency agreements.* 32 CFR part 2004 and E.O. 12829 require non-CSA agency heads to enter into agreements with the Secretary of Defense as the Executive Agent for the NISP to provide industrial security services. The Secretary of Defense may also enter into agreements to provide services for other CSA's in accordance with 32 CFR part 2004 and E.O. 12829. Agency agreements establish the terms of the Secretary of Defense's (or the Secretary of Defense's designee's) responsibilities when acting as the CSA on behalf of these agency heads. The list of agencies for which the Secretary of Defense has agreed to render industrial security services is on the DCSA website at *https://www.dcsa.mil.*

(l) *Security cognizance.* The CSA will inform contractors if oversight has been delegated to a CSO.

(m) *Rule interpretations.* Contractors will forward requests for interpretations of this rule to their CSA in accordance with their CSA-provided guidance to supplement unique CSA mission requirements.

(n) *Waivers to this rule.* Contractors will submit any requests to waive provisions of this rule in accordance with CSA procedures, which may include periodic review of approved waivers. When submitting a request for a waiver, the contractor will, in writing, explain why it is impractical or unreasonable for the contractor to comply with the requirement it is asking to waive, identify alternative measures as prescribed by this rule, and include a proposed duration for the waiver. The contractor cannot implement a waiver unless the waiver is approved by the applicable CSA.

(o) *Complaints and suggestions.* Contractors may forward NISP administration complaints and suggestions to the Director of ISOO. However, contractors are encouraged to forward NISP administration complaints and suggestions to their respective CSA prior to forwarding to the ISOO.

TABLE 2 TO PARAGRAPH (o) NISP ADMINISTRATION COMPLAINTS AND SUGGESTIONS

Addressee	Mailing address	Telephone No.	Facsimile	Email address
Director, ISOO, National Archives and Records Administration.	700 Pennsylvania Avenue NW, Room 100, Washington, DC 20408–0001.	202–357–5250	202–357–5907	*isoo@nara.gov.*

§ 117.8 Reporting requirements.

(a) *General.* Pursuant to this rule, Security Executive Agent Directive (SEAD) 3, (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-3-Reporting-U.pdf*) and CSA-provided guidance to supplement unique CSA mission requirements, contractors and their cleared employees are required to:

(1) Report certain events that may have an effect on the status of the entity's or an employee's eligibility for access to classified information; report events that indicate an insider threat to classified information or to employees with access to classified information; report events that affect proper safeguarding of classified information; and report events that indicate classified information has been, or is suspected to be, lost or compromised.

(2) Establish internal procedures to ensure employees with eligibility for access to classified information are aware of their responsibilities for reporting pertinent information to the FSO. The contractor will:

(i) Provide reports to the FBI, or other Federal authorities as required by this rule, the terms of a classified contract or other agreement, and by U.S. law.

(ii) Provide complete information to enable the CSA to ascertain whether classified information is adequately protected.

(iii) Submit reports to the FBI, the CSA, or the ISOO as specified in paragraphs (b), (c), and (g) of this section.

(3) Appropriately mark reports containing classified information in accordance with § 117.14.

(4) Clearly mark a report containing information submitted in confidence as containing that information. When reports contain information pertaining to an individual, 5 U.S.C. 552a (also known as and referred to in this rule as ''The Privacy Act of 1974, as amended,'') permits the withholding of certain information from the individual in accordance with specific exemptions, which include authority to withhold release of information to the extent that the disclosure of the information would reveal the identity of a source who furnished the information to the USG under an express promise that the identity of the source would be held in confidence.

(b) *Reports to be submitted to the FBI.* The contractor will promptly submit a written report to the nearest field office of the FBI regarding information coming to the contractor's attention concerning actual, probable, or possible espionage, sabotage, terrorism, or subversive activities at any of its locations.

(1) An initial report may be made by phone, but it must be followed up in writing (*e.g.,* email or formal correspondence), regardless of the FBI's disposition of the report.

(2) The contractor will promptly notify the CSA when they make a report to the FBI and provide the CSA a copy of the written report.

(c) *Reports to be submitted to the CSA.*—(1) *Adverse information.* Contractors are required to report adverse information coming to their attention concerning any of their employees determined to be eligible for access to classified information, in accordance with this rule, SEAD 3, and CSA-provided guidance. Contractors will not make reports based on rumor or innuendo.

(i) The termination of employment of an employee does not negate the requirement to submit this report. If a contractor employee is assigned to a USG location, the contractor will furnish a copy of the report and its final disposition to the USG security point of contact for that location.

(ii) Pursuant to *Becker* v. *Philco,* 372 F.2d 771 (4th Cir. 1967), cert. denied 389 U.S. 979 (1967), and subsequent cases, a contractor may not be liable for defamation of an employee because of communications that are required of and made by a contractor to an agency of the United States under the requirements of this rule or under the terms of applicable contracts.

(2) *Suspicious contacts.* Contractors will report information pertaining to suspicious contacts with employees determined to be eligible for access to classified information, and pertaining to efforts to obtain illegal or unauthorized access to the contractor's cleared facility by any means, including:

(i) Efforts by any individual, regardless of nationality, to obtain illegal or unauthorized access to classified information.

(ii) Efforts by any individual, regardless of nationality, to elicit information from an employee determined eligible for access to classified information, and any contact which suggests the employee may be the target of an attempted exploitation by an intelligence service of another country. See SEAD 3 for specific information to be reported.

(3) *Change in status of employees determined eligible for access to classified information.* Contractors will report by means of the CSA-designated reporting mechanism information pertaining to changes in status of employees determined eligible for access to classified information such as:

(i) Death.

(ii) Change in name.

(iii) Termination of employment.

(iv) Change in citizenship.

(4) *Citizenship by naturalization.* Contractors will report if a non-U.S. citizen employee granted an LAA becomes a citizen through naturalization. The report will include:

(i) City, county, and state where naturalized.

(ii) Date naturalized.

(iii) Court.

(iv) Certificate number.

(5) *Employees desiring not to be processed for a national security eligibility determination or not to perform classified work.* Contractors will report instances when an employee no longer wishes to be processed for a determination of eligibility for access to classified information or to continue having access to classified information, and the reason for that request.

(6) *Classified information nondisclosure agreement (NDA).* Contractors will report the refusal by an employee to sign the SF 312, ''Classified Information Nondisclosure Agreement,'' (available at: *https://www.gsa.gov/cdnstatic/SF312-13.pdf?forceDownload=1*) or other approved NDA.

(7) *Changed conditions affecting the contractor's eligibility for access to classified information.* Contractors are required to report certain events that affect the status of the entity eligibility determination (*e.g.,* FCL), affect the status of an employee's PCL, may indicate an employee poses an insider threat, affect the proper safeguarding of classified information, or indicate classified information has been lost or compromised, including:

(i) Change of ownership or control of the contractor, including stock transfers that affect control of the entity.

(ii) Change of operating name or address of the entity or any of its locations determined eligible for access to classified information.

(iii) Any change to the information previously submitted for KMP including, as appropriate, the names of the individuals the contractor is replacing. A new complete KMP listing need be submitted only at the discretion of the contractor or when requested by the CSA. The contractor will provide a statement indicating:

(A) Whether the new KMP are cleared for access to classified information, and if cleared, to what level they are cleared and when they were cleared, their dates and places of birth, social security numbers, and citizenship.

(B) Whether they have been excluded from access to classified information in accordance with § 117.7(b)(5)(ii).

(C) Whether they have been temporarily excluded from access to classified information pending the determination of eligibility for access to classified information in accordance with § 117.9(g).

(iv) Any action to terminate business or operations for any reason, imminent adjudication or reorganization in bankruptcy, or any change that might affect the validity of the contractor's eligibility for access to classified information.

(v) Any material change concerning the information previously reported concerning foreign ownership, control, or influence (FOCI). This report will be made by the submission of an updated SF 328, ''Certificate Pertaining to Foreign Interests,'' in accordance with CSA-provided guidance. When submitting this information, it is not necessary to repeat answers that have not changed. When entering into discussion, consultations, or agreements that may reasonably lead to effective ownership or control by a foreign interest, the contractor will report the details to the CSA in writing. If the contractor has received a Schedule 13D from the investor, the contractor will forward a copy with the report.

(8) *Changes in storage capability.* The contractor will report any changes in their storage requirement or capability to safeguard classified material.

(9) *Inability to safeguard classified material.* The contractor will report any emergency situation that renders their location incapable of safeguarding classified material as soon as possible.

(10) *Unsatisfactory conditions of a prime or subcontractors.* (i) Prime contractors, including subcontractors who have in turn subcontracted work, will report any information coming to their attention that may indicate that classified information cannot be adequately protected by a subcontractor, or other circumstances that may impact the validity of the eligibility for access to classified information of any subcontractors.

(ii) Subcontractors will report any information coming to their attention that may indicate that classified information cannot be adequately protected or other circumstances that may impact the validity of the eligibility for access to classified information of their prime contractor.

(11) *Dispositioned material previously terminated.* The contractor will make a report when the location or disposition of material previously terminated from accountability is subsequently discovered and brought back into accountability.

(12) *Foreign classified contracts.* Contractors will report any pre-contract negotiation or award not placed through a CSA or U.S. GCA that involves, or may involve:

(i) The release or disclosure of U.S. classified information to a foreign interest.

(ii) Access to classified information furnished by a foreign interest.

(13) *Reporting of improper receipt of foreign government material.* The contractor will report to the CSA the receipt of classified material from foreign interests that is not received through USG channels.

(14) *Reporting by subcontractor.* Subcontractors will also notify their prime contractors if they make any reports to their CSA in accordance with the provisions of paragraphs (c)(7) through (c)(10) of this section.

(d) *Reports of loss, compromise, or suspected compromise.* The contractor will report any loss, compromise, or suspected compromise of classified information, U.S. or foreign, to the CSA in accordance with paragraph (d)(1) through (d)(3) of this section. Each CSA may provide additional guidance concerning the reporting time period. If the contractor is located on a USG facility, the contractor will submit the report to the CSA and to the head of the USG facility.

(1) *Preliminary inquiry.* Immediately upon receipt of a security violation report involving classified information, the contractor will initiate a preliminary

inquiry to ascertain all of the circumstances surrounding the presumed loss, compromise, or suspected compromise, including validation of the classification of the information.

(2) *Initial report.* If the contractor's preliminary inquiry confirms that a loss, compromise, or suspected compromise of any classified information occurred, the contractor will promptly submit an initial report of the incident unless otherwise notified by the CSA.

(3) *Final report.* When the investigation has been completed, the contractor will submit a final report to the CSA which, in turn, will follow CSA procedures to notify the applicable GCA. The report will include:

(i) Material and relevant information that was not included in the initial report.

(ii) The full name and social security number of the individual or individuals primarily responsible for the incident, including a record of prior loss, compromise, or suspected compromise for which the individual had been determined responsible.

(iii) A statement of the corrective action taken to preclude a recurrence.

(iv) Disciplinary action taken against the responsible individual or individuals, if any.

(v) Specific reasons for reaching the conclusion that loss, compromise, or suspected compromise occurred or did not occur.

(4) *Employee information in compromise cases.* When requested by the CSA, the contractor will report information concerning an employee or other individual, determined to be responsible for the incident, when the information is needed by the CSA for the loss, compromise, or suspected compromise of classified information.

(e) *Individual culpability reports.* Contractors will establish and enforce policies that provide for appropriate administrative or disciplinary actions taken against employees who violate the requirements of this rule.

(1) Contractors will establish a system to manage and track information regarding employees with eligibility for access to classified information who violate the requirements of this rule in order to be able to identify patterns of negligence or carelessness, or to identify a potential insider threat.

(2) Contractors will establish and apply a graduated scale of administrative and disciplinary actions in the event of employee security violations or negligence in the handling of classified information. CSAs may provide guidance to contractors with examples of administrative or disciplinary actions that the contractor may consider implementing in the event of employee violations or negligence. Contractors are required to submit a final report to the CSA with the findings of an employee's culpability and what corrective actions were taken.

(3) Contractors will include a statement of the administrative or disciplinary actions taken against an employee in a final report to the CSA. A statement must be included when the individual responsible for a security violation can be determined. Contractors' final reports will indicate whether one or more of the following factors are evident:

(i) Involved a deliberate disregard of security requirements.

(ii) Involved negligence in the handling of classified material.

(iii) Was not deliberate in nature but reflects a recent or recurring pattern of questionable judgment, irresponsibility, negligence, or carelessness.

(f) *CDC cyber incident reports.* This paragraph applies only to CDCs and sets forth reporting requirements pursuant to 10 U.S.C. 391 and 393 and Defense Federal Acquisition Regulation Supplement Clause 252.204–7012. The reporting requirements of paragraph (f) of this section are in addition to the requirements in paragraphs (b) and (d) of this section, which can include certain activities occurring on unclassified information systems. DoD will provide detailed reporting instructions for contractors affected by these references via industrial security letter in accordance with DoDI 5220.22.

(1) *Reports to be submitted to the designated DoD CSO.* CDCs will immediately report to the DoD CSO, any cyber incident on a classified covered information system that has been approved by that CSO to process classified information.

(i) At a minimum, the report will include:

(A) A description of the technique or method used in the cyber incident.

(B) A sample of the malicious software involved in the cyber incident, if discovered and isolated by the CDC,

(C) A summary of information in connection with any DoD program that has been potentially compromised due to the cyber incident.

(ii) Information that is reported by the CDC (or derived from information reported by the CDC) will be safeguarded, used, and disseminated in a manner consistent with DoD procedures governing the handling of such information pursuant to Public Law 112–239 and 10 U.S.C. 391.

(iii) Reports involving classified foreign government information will be reported to the Director, Defense Technology Security Administration (DoD).

(2) *Reports on non-Federal information systems not authorized to process classified information.* CDCs will report cyber incidents on non-Federal, unclassified information systems in accordance with contract requirements.

(3) *Access to equipment and information by DoD personnel.* (i) The CDC will allow, upon request by DoD personnel, access by DoD personnel to additional equipment or information of the CDC that is necessary to conduct forensic analysis of reportable cyber incidents in addition to any analysis conducted by the CDC.

(ii) The CDC is only required to provide DoD access to equipment or information to determine whether information created by or for DoD in connection with any DoD program was successfully exfiltrated from a CDC's network or information system, and what information was exfiltrated from the CDC's network or information system.

(g) *Reports to ISOO.* (1) Contractors will report instances of redundant or duplicative security review and audit activity by the CSAs to the Director, ISOO, for resolution.

(2) Contractors will report instances of CSAs duplicating processing to determine an entity's eligibility for access to classified information when there is an existing determination of an entity's eligibility for access to classified information by another CSA.

§ 117.9 Entity eligibility determination for access to classified information.

(a) *General.* This section applies to all contractors with entity eligibility determinations, except as provided in § 117.22 for entity eligibility determinations for participation in the CCIPP under the cognizance of DHS.

(1) Prior to the entity being granted an entity eligibility determination for access to classified information, the responsible CSA must have determined that:

(i) The entity is eligible for access to classified information to meet a legitimate USG or foreign government need.

(ii) Access is consistent with national security interests.

(2) The CSA will provide guidance on processing entity eligibility determinations for entity access to classified information.

(3) The determination of entity eligibility for access is separate from the determination of a classified

information safeguarding capability (see § 117.15).

(4) Neither the contractor nor its employees will be permitted access to classified information until the CSA has made an entity eligibility determination (*e.g.,* issued an FCL).

(5) The requirement for a favorable entity eligibility determination (also referred to in some instances as an FCL) for a prime contractor includes instances where all access to classified information will be limited to subcontractors. A prime contractor must have a favorable entity eligibility determination at the same or higher classification level as its subcontractors.

(6) Contractors are eligible for storage of classified material in connection with a legitimate USG or foreign government requirement if they have a favorable entity eligibility determination and a classified information safeguarding capability approved by the CSA.

(7) An entity eligibility determination is valid for access to classified information at the same or lower classification level.

(8) Each CSA will maintain a record of entity eligibility determinations made by that CSA.

(9) A contractor will not use its favorable entity eligibility determination for advertising or promotional purposes. This does not prohibit the contractor from advertising employee positions that require a PCL in connection with the position.

(10) A contractor or prospective contractor cannot apply for its own entity eligibility determination. A GCA or a currently cleared contractor may sponsor an entity for an entity eligibility determination at any point during the contracting or agreement life cycle at which the entity must have access to classified information to participate (including the solicitation or competition phase).

(b) *Reciprocity.* If an entity has an appropriate, final entity eligibility determination, a CSA will not duplicate the entity eligibility determination processes performed by another CSA. If a CSA cannot acknowledge an entity eligibility determination to another CSA, the involved entity may be subject to duplicate processing in accordance with 32 CFR part 2004.

(c) *Eligibility requirements.* To be eligible for an initial entity eligibility determination or to maintain an existing entity eligibility determination, the entity must:

(1) Need access to classified information in connection with a legitimate USG or foreign government requirement, and access must be consistent with U.S. national security interests as determined by the CSA.

(2) Be organized and existing:

(i) Under the laws of the United States, one of the fifty States, the District of Columbia, or an organized U.S. territory (Guam, Commonwealth of the Northern Marianas Islands, Commonwealth of Puerto Rico, and the U.S. Virgin Islands); or

(ii) Under the laws of an American Indian/Alaska Native tribal entity if:

(A) The American Indian or Alaska Native tribe under whose laws the entity is chartered has been formally acknowledged by the Assistant Secretary—Indian Affairs, of the U.S. Department of the Interior.

(B) The contractor is organized and continues to exist, during the period of the eligibility under a tribal statue or code, or pursuant to a resolution of an authorized tribal legislative body.

(C) The contractor has submitted or will submit records such as a charter, certificate of organization, or other applicable tribal documents and statute or code provisions governing the formation and continuation of the entity, for CSA determination that the entity is tribally chartered.

(3) Be located in the United States or its territorial areas.

(4) Have a record of integrity and lawful conduct in its business dealings.

(5) Have a SMO, FSO, and ITPSO who have and who maintain eligibility for access to classified information and are not excluded from participating in USG contracts or agreements in accordance with § 117.7(b)(1) through § 117.7(b)(3).

(6) Not be under FOCI to such a degree that a favorable entity eligibility determination for access to classified information would be inconsistent with the national interest, in the judgment of the CSA.

(7) Maintain sufficient authorized and cleared employees to manage and implement the requirements of this rule in accordance with CSA guidance.

(8) Not pose an unacceptable risk to national security interests, in the judgment of the CSA.

(9) Meet all requirements governing access to classified information established by the CSA or the relevant authorizing law, regulation, or government-wide policy.

(d) *Processing the entity eligibility determination.* The CSA will assess the entity's eligibility for access to classified information based on its business structure.

(1) At a minimum, the entity will:

(i) Provide CSA-requested documentation within timelines established by the CSA.

(ii) Have and identify the SMO.

(iii) Appoint a U.S. citizen employee as the FSO.

(iv) Appoint a U.S. citizen employee as the ITPSO.

(v) Submit requests for personnel security investigations for the SMO, FSO, ITPSO, and those other KMP identified by the CSA as requiring eligibility for access to classified information in connection with the entity eligibility.

(2) If the entity is under FOCI with a special security agreement (SSA) as the proposed method of FOCI mitigation, and the GCA requires the entity to have access to proscribed information, the CSA must consider the measures listed in § 117.11(d) as part of the entity eligibility determination.

(e) *Other personnel eligibility determinations concurrent with the entity eligibility determination.* (1) Contractors may designate employees who require access to classified information during the negotiation of a contract or the preparation of a bid or quotation pertaining to a prime contract or a subcontract. These designated employees will be processed for a determination of eligibility for access to classified information (*i.e.,* PCL eligibility) concurrent with entity's entity eligibility determination.

(2) The entity eligibility determination is not dependent on the PCL eligibility for access to classified information by such employees, provided none of these employees are among those listed in paragraph (c)(5) of this section. Even so, the employees will not be granted access to classified information until both a favorable entity eligibility determination and PCL eligibility has been granted.

(f) *Exclusion procedures.* If a CSA determines that certain KMP can be excluded from access to classified information, the contractor will follow the procedures in accordance with § 117.7(b)(5)(ii).

(g) *Temporary exclusions.* As a result of a changed condition, the SMO or other KMP who require eligibility for access to classified information in connection with the facility entity eligibility determination may be temporarily excluded from access to classified information while in the process of a PCL eligibility determination provided:

(1) The SMO or other KMP are not appointed as the FSO or ITPSO. FSOs and ITPSOs may not be temporarily excluded. A cleared employee must always be appointed to fulfill the requirements of these positions in accordance with this rule.

(2) An employee, cleared to the level of the entity eligibility determination,

must be able to fulfill the NISP responsibilities of the temporarily excluded KMP in accordance with this rule while the temporary exclusion is in effect.

(3) The applicable CSA may provide additional guidance on the duration of a temporary exclusion from access to classified information based on circumstances, business structure, and other relevant security information.

(4) The contractor's governing board affirms the exclusion action, and provides a copy of the exclusion action to the CSA. The organization's governing body will document this action.

TABLE 1 TO PARAGRAPH (g)(4) TEMPORARY EXCLUSION RESOLUTIONS

Type of affirmation	Language to be used in exclusion action
Affirmation for Temporary Exclusion from Access to Classified Information.	Pending a final determination of eligibility for access to classified information by the U.S. Government, [insert name and position] will not require, will not have, and can be effectively and formally excluded from access to all classified information disclosed to the entity.
Affirmation for Temporary Exclusion from Higher Level Classified Information.	Pending a final determination of eligibility for access to classified information at the [insert SECRET or TOP SECRET] level, [insert name and position] will not have, and can be effectively and formally excluded from access to higher-level classified information [specify which higher level of information].

(h) *Interim entity eligibility determinations.* The CSA may make an interim entity eligibility determination for access to classified information, in the sole discretion of the CSA. See § 117.10(l) for access limitations that also apply to interim entity eligibility determinations.

(i) An interim entity eligibility determination is made on a temporary basis pending completion of the full investigative requirements.

(ii) If the contractor with an interim entity eligibility determination is unable or unwilling to comply with the requirements of this rule and CSA-provided guidance regarding the process to obtain a final entity eligibility determination, the CSA will withdraw the interim entity eligibility.

(i) *Multiple facility organizations.* The home office must have an entity eligibility determination at the same level as the highest entity eligibility determination of an entity within the MFO. The CSA will determine whether branch offices are eligible for access to classified information if the branch offices need access and meet all other requirements.

(j) *Parent-subsidiary relationships.* When a parent-subsidiary relationship exists, the CSA will process the parent and the subsidiary separately for entity eligibility determinations.

(1) If the CSA determines the parent must be processed for an entity eligibility determination, then the parent must have an entity eligibility determination at the same or higher level as the subsidiary.

(2) When a parent and subsidiary or multiple cleared subsidiaries are collocated, a formal written agreement to use common security services may be executed by the entities, subject to the approval of the CSA.

(k) *Joint ventures.* A joint venture may be granted eligibility for access to classified information if it meets the eligibility requirements in paragraph (c) of this section, including:

(1) The joint venture must be established as a legal business entity (*e.g.* limited liability company, corporation, or partnership). A joint venture established by contract that is not also established as a legal business entity is not eligible for an entity eligibility determination.

(2) The business entity operating as a joint venture must have been awarded a classified contract or sponsored by a GCA or prime contractor for an entity eligibility determination in advance of a potential award for which the business entity has bid pursuant to paragraph (c) of this section.

(3) The business entity operating as a joint venture must have an employee or employees appointed as security officials or KMP pursuant to § 117.7(b).

(l) *Consultants.* The responsible CSA will determine when there is a need for self-employed consultants requiring access to classified information to be considered for an entity eligibility determination.

(m) *Limited entity eligibility determination (Non-FOCI).* (1) The applicable CSA may choose to allow a GCA to request limited entity eligibility determinations for a single, narrowly defined contract, agreement, or circumstance and specific to the requesting GCA's classified information. This is not the same as a limited entity eligibility determination in situations involving FOCI, when the FOCI is not mitigated or negated.

(i) Limited entity eligibility determinations (or FCLs) involving FOCI will be processed in accordance with § 117.11(e).

(ii) This paragraph (paragraph (m) of this section) applies to limited entity eligibility determinations for purposes other than FOCI mitigation in accordance with 32 CFR part 2004. Additional guidance may be provided by the responsible CSA.

(2) An entity must be sponsored for a limited entity eligibility determination by a GCA in accordance with the sponsorship requirements contained in paragraph (c) of this section. The contractor should be aware that the sponsorship request from the GCA to the CSA must also include:

(i) Description of the compelling need for the limited entity eligibility determination that is in accordance with U.S. national security interests.

(ii) Specific reason(s) or rationale for limiting the entity eligibility determination.

(iii) The GCA's formal acknowledgement and acceptance of the risk associated with this rationale.

(3) The entity must otherwise meet the entity eligibility determination requirements set out in this rule.

(4) Access limitations are inherent with the limited entity eligibility determination and are imposed upon all of the entity's employees regardless of citizenship.

(5) Contractors should be aware that the CSA will document the requirements of each limited entity eligibility determination it makes, including the scope of, and any limitations on, access to classified information.

(6) Contractors should be aware that the CSA will verify limited entity eligibility determinations only to the requesting GCA. In the case of multiple limited entity eligibility determinations for a single entity, the CSA verifies each one separately only to its requestor.

(7) The applicable CSA administratively terminates the limited entity eligibility determination when there is no longer a need for access to the classified information for which the CSA approved the limited entity eligibility determination.

(n) *Termination of the entity eligibility determination.* Once granted, a favorable entity eligibility determination remains in effect until terminated or revoked. If the entity eligibility determination is terminated or revoked, the contractor will return all classified material in its possession to the appropriate GCA or dispose of the material as instructed by the CSA. The contractor should be aware that it may request an administrative termination or the CSA may:

(1) After coordination with applicable GCAs, administratively terminate the entity eligibility determination because the contractor no longer has a need for access to classified information.

(2) Revoke an entity eligibility determination if the contractor is unable or unwilling to protect classified information or is unable to comply with the security requirements of this rule.

(o) *Invalidation of the entity eligibility determination.* The CSA may invalidate an existing entity eligibility determination. While the entity eligibility determination is in an invalidated status, the contractor may not bid on or be awarded new classified contracts or solicitations. The contractor may continue to work on existing classified contracts if the GCA agrees.

(p) *Records maintenance.* Contractors will maintain the original CSA designated forms for the duration of the entity eligibility determination in accordance with CSA-provided guidance.

§ 117.10 Determination of eligibility for access to classified information for contractor employees.

(a) *General.* (1) The CSA is responsible for determining an employee's eligibility for access to classified information.

(i) The contractor must determine that access to classified information is essential in the performance of tasks or services related to the fulfillment of a classified contract.

(ii) Access must be clearly consistent with U.S. national security interests as determined by the CSA.

(iii) A contractor may give an employee access to classified information at the same or lower level of classification as the level of the contractor's entity eligibility determination if the employee has:

(A) A valid need-to-know for the classified information.

(B) A USG favorable eligibility determination for access to classified information at the appropriate level; and

(C) Signed a non-disclosure agreement.

(2) The CSA will determine eligibility for access to classified information in accordance with SEAD 4 (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-4-Adjudicative-Guidelines-U.pdf*) and notify the contractor when eligibility has been granted.

(i) The CSA will notify the contractor when an employee's eligibility has been denied, suspended, or revoked.

(ii) The contractor will immediately deny access to classified information to any employee when notified of a denial, revocation, or suspension of eligibility regardless of the contractor employee's location.

(iii) If the employee's performance is at a USG facility, the contractor will provide notification to the appropriate GCA of any denial, revocation, or suspension of eligibility for access to classified information.

(3) Contractors will annotate and maintain the accuracy of their employees' records in the system of record for contractor eligibility and access to classified information, when one has been designated by the CSA.

(4) Within an MFO or within the same business organization, contractors may centrally manage eligibility for access to classified information and access to classified information records.

(5) The contractor will limit requests for determinations of eligibility for access to classified information to the minimum number of employees and consultants necessary for operational efficiency in accordance with contractual obligations and other requirements of this rule. Requests for determinations of eligibility for access to classified information will not be used to establish a cache of cleared employees.

(6) The contractor will not submit a request for an eligibility determination to one CSA if the employee applicant is known to be cleared or in process for eligibility for access to classified information by another CSA. In such cases, reciprocity of eligibility determination in accordance with SEAD 7 (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf*) shall be used. The contractor will provide the new CSA with the full name, date, and place of birth, social security number, clearing agency, and type of investigation for verification.

(7) Contractors will not submit requests for determination of eligibility for access to classified information for individuals who are not their employees or consultants; nor will they submit requests for employees of subcontractors.

(8) Access to SCI, SAP, FRD, and RD information is a determination made by the granting authority by the applicable USG granting authority for each category of information.

(b) *Investigative requirements.* E.O. 13467, as amended, ''Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information,'' designates the Security and Suitability Executive Agents responsible for establishing the standards for investigative requirements that apply to contractors.

(1) *Investigative tiers.* The standards established in accordance with E.O. 13467, as amended, designate specific investigative tiers that are acceptable for access to classified information. An investigative tier is for positions designated as moderate risk, non-critical sensitive, and allow access to information classified at the L, CONFIDENTIAL, and SECRET levels. Another investigative tier is for positions designated as high risk, critical sensitive, special sensitive, and allow access to information classified at the Q, TOP SECRET, and SCI levels.

(2) *Investigative coverage.* (i) *Automated sources.* Investigative providers will use automation whenever possible to collect, verify, corroborate, or discover information about an individual, as documented on the request for investigation or developed from other sources, *i.e.,* automated record checks and inquiries.

(ii) *Interviews.* Interviews, if required, will cover areas of adjudicative concern.

(iii) *Information Covered in Previous Investigations.* Information validated in a prior investigation, the results of which are not expected to change (*e.g.,* verification of education degree), will not be repeated as part of subsequent investigations.

(3) *Polygraph.* Agencies with policies authorizing the use of the polygraph for purposes of determining eligibility for access to classified information may require polygraph examinations when necessary. If adjudicatively relevant information arises during the investigation or the polygraph examination, the investigation may be expanded to resolve the adjudicative concerns.

(4) *Financial disclosure.* When a GCA requires that a contractor employee complete a financial disclosure form, the contractor will ensure that the employee has the opportunity to complete and submit the form in accordance with the Privacy Act of 1974, as amended, and other applicable provisions of law.

(5) *Reinvestigation and Continuous Evaluation.* Contractor employees

determined eligible for access to classified information will follow CSA guidance to complete reinvestigation and continuous evaluation or continuous vetting requirements. The contractor will validate that the employee requires continued eligibility for access to classified information before initiating the reinvestigation.

(c) *Verification of U.S. citizenship.* A contractor will require each applicant for determination of eligibility for access to classified information who claims U.S. citizenship to provide evidence of citizenship to the FSO or other authorized representative of the contractor. All documentation must be the original or certified copies of the original documents.

(1) Any document, or its successor, listed in this paragraph is an acceptable document to corroborate U.S. citizenship by birth, including by birth abroad to a U.S. citizen.

(i) A birth certificate certified with the registrar's signature, which bears the raised, embossed, impressed, or multicolored seal of the registrar's office.

(ii) A current or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.

(iii) A Department of State Form FS–240, ''Consular Report of Birth Abroad of a Citizen of the United States of America.''

(iv) A Department of State Form FS–545 or DS–1350, ''Certification of Report of Birth.''

(2) Any document, or its successor, listed in this paragraph is an acceptable document to corroborate U.S. citizenship by certification, naturalization, or birth abroad to a U.S. citizen.

(i) A U.S. Citizenship and Immigration Services Form N–560 or N–561, ''Certification of U.S. Citizenship.''

(ii) A U.S. Citizenship and Immigration Services Form 550, 551, or 570, ''Naturalization Certificate.''

(iii) A valid or expired U.S. passport or passport card that is unaltered and undamaged and was originally issued to the individual.

(d) *Procedures for completing the electronic version of the SF 86,* ''*Questionnaire for National Security Positions.*'' The electronic version of the SF 86 (available at: *https://www.opm.gov/forms/pdf_fill/sf86.pdf*) must be completed in e-QIP or its successor system by the contractor employee and reviewed by the FSO or other contractor employee(s) who has (have) been specifically designated by the contractor to review an employee's SF 86. The FSO or designee will:

(1) Provide the employee with written notification that review of the SF 86 by the FSO or other contractor employee is for adequacy and completeness and information will be used for no other purpose within the entity. The use and disclosure by the U.S. Government, and by U.S. Government contractors operating systems of records on behalf of a U.S. Government agency to accomplish an agency function, of the information provided by the employee on the SF–86 is governed by the Privacy Act of 1974, as amended, and by the routine uses published by the USG in the applicable System of Records Notice.

(2) Not share information from the employee's SF 86 within the entity and will not use the information for any purpose other than determining the adequacy and completeness of the SF 86.

(e) *Fingerprint collection.* The contractor will submit fingerprints in accordance with CSA guidance. Contractors will use digital fingerprints whenever possible.

(f) *Pre-employment eligibility determination action.* (1) If a potential employee requires access to classified information immediately upon commencement of employment, the contractor may submit a request for investigation prior to the date of employment, provided:

(i) A written commitment for employment has been made by the contractor.

(ii) The candidate has accepted the offer in writing.

(2) The commitment for employment must indicate employment will commence within 45 days of the employee being granted eligibility for access to classified information at a level that allows them to perform the tasks or services associated with the contract or USG requirement for which they were hired.

(3) Contractors will comply with the requirements pursuant to paragraph (a)(5) of this section.

(g) *Classified information NDA.* The NDA designated by the CSA (*e.g.,* SF 312), is an agreement between the USG and an individual who is determined eligible for access to classified information.

(1) An employee determined eligible for access to classified information must execute an NDA prior to being granted access to classified information.

(2) The employee must sign and date the NDA in the presence of a witness. The employee's and witness' signatures must bear the same date.

(3) The contractor will forward the executed NDA to the CSA for retention. The CSA may authorize the contractor to retain a copy of the form for administrative purposes, if appropriate.

(4) If the employee refuses to execute the NDA, the contractor will deny the employee access to classified information and submit a report to the CSA in accordance with § 117.8(c)(6).

(h) *Reciprocity.* The applicable CSA is responsible for determining whether contractor employees have been previously determined eligible for access to classified information or investigated by an authorized investigative activity in accordance with SEAD 7 (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-7_BI_ReciprocityU.pdf*).

(1) Any current eligibility determination for access to classified information that is based on an investigation of a scope that meets or exceeds that necessary for the required level of access will provide the basis for a new eligibility determination.

(2) The prior investigation will be used without further investigation or adjudication unless the CSA becomes aware of significant derogatory information that was not previously adjudicated.

(i) *Break in access.* There are circumstances when a contractor administratively terminates an employee's access to classified information solely because of no current requirement for such access. If the employee again requires access to classified information and has been in the contractor's continuous employment, and the employee again requires access to classified information, the contractor may provide access to classified information without further investigation, based on CSA guidance, so long as the employee remains eligible for access to classified information and has a current investigation of a scope that meets or exceeds that necessary for the access required and no new derogatory information is known. Any adverse information from or about the employee must continue to be reported while the employee maintains eligibility for access to classified information, even when access to classified information has been administratively terminated.

(j) *Break in employment.* (1) When an employee had a break in employment and now requires access to classified information, the contractor may provide access to classified information based on CSA guidance provided the employee remains eligible for access to classified information and has a current investigation of a scope that meets or exceeds that necessary for the access required.

(2) The contractor may not provide access to classified information to an employee who previously was eligible for access to classified information, but has had a break in employment that resulted in a loss of eligibility without a new eligibility determination by the CSA.

(k) *Non-U.S. citizens.* (1) Contractors must make every effort to ensure that non-U.S. citizens are not employed in duties that may require access to classified information. However, compelling reasons may exist to grant access to classified information to a non-U.S. citizen. The CSA may grant such individuals a LAA in those rare circumstances where a non-U.S. citizen possesses unique or unusual skills or expertise that is urgently needed to support a specific USG contract involving access to specified classified information, and a cleared or clearable U.S. citizen is not readily available. The CSA will provide specific procedures for requesting an LAA, to include the need for approval by a GCA senior official.

(2) An LAA granted under the provisions of this rule is not valid for access to:

(i) TOP SECRET information.

(ii) RD or FRD.

(iii) Information that has not been determined releasable by a USG designated disclosure authority to the country of which the individual is a citizen.

(iv) Communications security (COMSEC) information.

(v) Intelligence information.

(vi) NATO information. Foreign nationals of a NATO member nation may be authorized access to NATO information provided:

(A) The CSA obtains a NATO security clearance certificate from the individual's country of citizenship.

(B) NATO access is limited to performance on a specific NATO contract.

(vii) Information for which foreign disclosure has been prohibited in whole or in part.

(viii) Information provided to the USG in confidence by a third-party government.

(ix) Classified information furnished by a third-party government.

(l) *Temporary eligibility for access to classified information.* In accordance with SEAD 8 (available at: *https://www.dni.gov/files/NCSC/documents/Regulations/SEAD-8_Temporary_Eligibility_U.pdf*), the CSA may grant temporary (previously called interim) eligibility for access to classified information, as appropriate, to applicants for access to TOP SECRET, SECRET, and CONFIDENTIAL information. This eligibility may only be granted if there is no evidence of adverse information that calls into question an individual's eligibility for access to classified information. If results are favorable following completion of full investigative requirements, the CSA will update the temporary eligibility determination for access to classified information to be final. In any case, a temporary eligibility determination shall not exceed one year unless approved by the applicable CSA in the system of record. Non-U.S. citizens are not eligible for access to classified information on a temporary basis.

(1) A temporary SECRET or CONFIDENTIAL eligibility determination is valid for access to classified information at the level of the eligibility granted. Access to RD, COMSEC information, and NATO information requires a final SECRET eligibility determination.

(2) A temporary TOP SECRET eligibility determination is valid for access to TOP SECRET information. If an individual has a temporary TOP SECRET eligibility determination and has a final SECRET eligibility determination based on a previously completed investigation, the temporary TOP SECRET eligibility determination is valid for access to RD, NATO, and COMSEC information at the SECRET or CONFIDENTIAL level.

(3) Access to SCI and SAP information based on a temporary eligibility determination is a determination made by the granting authority.

(4) When a temporary eligibility determination has been made and derogatory information is subsequently developed, the CSA may withdraw the temporary eligibility pending completion of the processing that is a prerequisite to the final eligibility determination.

(5) When a temporary eligibility determination is withdrawn for an individual who is required to be eligible for access to classified information in connection with the entity eligibility determination for access to classified information, the contractor must remove the individual from access to classified information and any KMP position requiring PCL eligibility or the temporary entity eligibility determination will also be withdrawn.

(6) Withdrawal of a temporary eligibility determination is not a denial, termination, or revocation of eligibility under this rule and may not be appealed.

(m) *Consultants.* (1) A consultant will not access classified information off the premises of the using (hiring) contractor except in connection with authorized classified visits.

(2) A contractor may only assign a consultant outside the United States with responsibilities requiring access to classified information when:

(i) The consultant agreement between the contractor and consultant includes:

(A) Identification of the contract, license, or agreement that requires access to classified information, the level of classified information that is required, and access to FGI by the consultant while assigned outside the United States.

(B) A formal agreement that prohibits the consultant from disclosing any classified information related to the contract, license, or agreement as required in paragraph (m)(i)(A) of this section to any party other than the USG or foreign government with which the consultant is meeting, and who possesses the requisite clearance and need to know.

(ii) The consultant and the using contractor will jointly execute the consultant agreement setting forth respective security responsibilities. The contractor will retain an original signed copy of the agreement and will ensure its availability if requested by the CSA.

(iii) The contractor, in consultation with the applicable CSA as appropriate, will determine what threat briefing(s) the consultant should receive before the assignment, and conduct those briefings as part of the consultant's pre-assignment and recurring security training.

(iv) The contractor provides notice of any changes to the consultant agreement to the applicable CSA during assessments or upon CSA request.

(3) The using contractor will be the consumer of the consultant services as set forth in the consultant agreement.

(4) For security administration purposes, a consultant will be considered an employee of the using contractor for compliance with this rule.

(5) Consultants to GCAs are not under the purview of the NISP and will be processed for determination of eligibility by the GCA in accordance with GCA procedures.

§ 117.11 Foreign Ownership, Control, or Influence (FOCI).

(a) *General.* Foreign investment can play an important role in maintaining the vitality of the U.S. industrial base. Therefore, it is the intent of the USG to allow foreign investment consistent with the national security interests of the United States. The following FOCI

procedures for cleared U.S. entities are intended to mitigate the risks associated with FOCI by ensuring that foreign firms cannot undermine U.S. security to gain unauthorized access to classified information.

(1) The CSA will consider a U.S. entity to be under FOCI when:

(i) A foreign interest has the power to direct or decide issues affecting the entity's management or operations in a manner that could either:

(A) Result in unauthorized access to classified information; or

(B) Adversely affect performance of a classified contract or agreement.

(ii) The foreign government is currently exercising, or could prospectively exercise, that power, whether directly or indirectly, such as:

(A) Through ownership of the U.S. entity's securities, by contractual arrangements, or other means, or;

(B) By the ability to control or influence the election or appointment of one or more members to the entity's governing board.

(2) When the CSA has determined that an entity is under FOCI, the primary consideration will be the protection of classified information. The CSA will take whatever action is necessary to protect classified information, in coordination with other affected agencies as appropriate.

(3) A U.S. entity that is in process for an entity eligibility determination for access to classified information and subsequently determined to be under FOCI is ineligible for access to classified information unless and until effective security measures have been put in place to negate or mitigate FOCI to the satisfaction of the CSA.

(4) When a contractor determined to be under FOCI is negotiating an acceptable FOCI mitigation or negation measure in good faith, an existing entity eligibility determination may continue in effect so long as there is no indication that classified information is at risk of compromise in consultation with the applicable GCA. The applicable CSA may decide that circumstances involving the FOCI are such that the entity eligibility determination will be invalidated until implementation of an acceptable FOCI mitigation plan.

(5) An existing entity eligibility determination will be invalidated if the contractor is unable or unwilling to negotiate and implement an acceptable FOCI mitigation or negation measure. An existing entity eligibility determination will be revoked if security measures cannot be taken to remove the possibility of unauthorized access to classified information or adverse effect on performance of classified contracts.

(6) Changed conditions, such as a change in ownership, indebtedness, or a foreign intelligence threat, may justify certain adjustments to the security terms under which an entity is operating or, alternatively, that a different FOCI mitigation or negation method be employed. If a changed condition is of sufficient significance, it might also result in a determination that a contractor is no longer considered to be under FOCI, or, conversely, that a contractor is no longer eligible for access to classified information.

(7) The USG reserves the right, and has the obligation, to impose any security method, safeguard, or restriction (including denial, termination or revocation of an entity eligibility determination) it believes necessary to ensure that unauthorized access to classified information is effectively precluded and performance of classified contracts is not adversely affected.

(8) Nothing contained in this section affects the authority of a Federal agency head to limit, deny, or revoke access to classified information under its statutory, regulatory, or contract jurisdiction.

(b) *Factors.* Factors relating to the entity, relevant foreign interests, and the government of such foreign interests, as appropriate, will be considered in the aggregate to determine whether an applicant entity is under FOCI, its eligibility for access to classified information, and the protective measures required. These factors include:

(1) Record of espionage against U.S. targets, either economic or government.

(2) Record of enforcement actions against the entity for transferring technology without authorization.

(3) Record of compliance with pertinent U.S. laws, regulations, and contracts or agreements.

(4) Type and sensitivity of the information the entity would access.

(5) Source, nature, and extent of FOCI, including whether foreign interests hold a majority or minority position in the entity, taking into consideration the immediate, intermediate, and ultimate parent entities.

(6) Nature of any relevant bilateral and multilateral security and information exchange agreements.

(7) Ownership or control, directly or indirectly, in whole or in part, by a foreign government.

(8) Any other factor that indicates or demonstrates capability of foreign interests to control or influence the entity's operations or management.

(c) *Procedures.* An entity is required to complete an SF 328 during the process for an entity eligibility determination or when significant changes occur to information previously submitted. In the case of a corporate family, the form may be a consolidated response rather than separate submissions from individual members of the corporate family based on CSA guidance.

(1) If an entity provides any affirmative answers on the SF 328, or the CSA receives other information which indicates that the applicant entity may be under FOCI, the CSA will make a risk-based determination regarding the relative significance of the information in regard to:

(i) Whether the applicant is under FOCI.

(ii) The extent and manner to which the FOCI represents a risk to the national security or may adversely impact classified contract performance.

(iii) The type of actions, if any, that would be necessary to mitigate or negate the effects of FOCI to a level deemed acceptable to the USG. The CSA will advise entities on the CSA's appeal channels for disputing CSA FOCI determinations.

(2) When an entity with a favorable eligibility determination enters into negotiations for the proposed merger, acquisition, or takeover by a foreign interest, the entity will submit notification to the CSA of the commencement of such negotiations.

(i) The submission will include the type of transaction under negotiation (*e.g.,* stock purchase, asset purchase), the identity of the potential foreign interest investor, and a plan to negate or mitigate the FOCI by a method outlined in paragraph (d) of this section.

(ii) The entity will submit copies of loan, purchase, and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, other organizational documents, and reports filed with other Federal agencies to the CSA.

(d) *FOCI action plans.* (1) When FOCI factors not related to ownership are present, the CSA will determine if positive measures will assure the CSA that the foreign interest can be effectively mitigated and cannot otherwise adversely affect performance on classified contracts. Examples of such measures include:

(i) Modification or termination of loan agreements, contracts, and other understandings with foreign interests.

(ii) Diversification or reduction of foreign-source income.

(iii) Demonstration of financial viability independent of foreign interests.

(iv) Elimination or resolution of problem debt.

(v) Assignment of specific oversight duties and responsibilities to board members.

(vi) Formulation of special executive-level security committees to consider and oversee issues that affect the performance of classified contracts.

(vii) Physical or organizational separation of the contractor component performing on classified contracts.

(viii) Adoption of special board resolutions.

(ix) Other actions that negate or mitigate foreign control or influence.

(x) A combination of these methods, as determined by the CSA.

(2) When FOCI factors related to ownership are present, methods the CSA may apply to negate or mitigate the risk of foreign ownership include, but are not limited to:

(i) *Board resolution.* (A) When a foreign interest does not possess voting interests sufficient to elect, or otherwise is not entitled to representation on the entity's governing board, a resolution(s) by the governing board may be adequate. In the resolution, the governing board will:

(*1*) Identify the foreign shareholder.

(*2*) Describe the type and number of foreign-owned shares.

(*3*) Acknowledge the entity's obligation to comply with all industrial security program requirements.

(*4*) Certify that the foreign owner does not require, will not have, and can be effectively precluded from unauthorized access to all classified information entrusted to or held by the entity.

(B) The governing board will provide for annual certifications to the CSA acknowledging the continued effectiveness of the resolution.

(C) The entity will distribute to members of its governing board and to its KMP copies of such resolutions, and report in the entity's corporate records the completion of such distribution.

(ii) *Security control agreement (SCA).* When a foreign interest does not effectively own or control an entity (*i.e.,* the entity is under U.S. control), but the foreign interest is entitled to representation on the entity's governing board, an SCA may be adequate. At least one cleared U.S. citizen must serve as an outside director on the entity's governing board. There are no access limitations under an SCA.

(iii) *SSA.* When a foreign interest effectively owns or controls an entity, an SSA may be adequate. An SSA is an arrangement that, based upon an assessment of the source and nature of FOCI and FOCI factors, imposes various industrial security measures within an institutionalized set of entity practices and procedures. The SSA preserves the foreign owner's right to be represented on the entity's board or governing body with a direct voice in the entity's business management, while denying the foreign owner majority representation and unauthorized access to classified information.

(A) *Requirement for a National Interest Determination (NID).* Unless otherwise prohibited by law or regulation (*e.g.,* Section 842 of Pub. L. 115–232), the applicable CSA must determine whether allowing an entity access to proscribed information under an SSA is consistent with national security interests of the U.S. with concurrence from controlling agencies, as applicable. Such NIDs will be made as part of an entity eligibility determination or because of a changed condition when a GCA requires an entity to have access to proscribed information and the CSA proposes an SSA as the mitigation measure. The NID can be program, project, or contract specific.

(B) *NID process:* (*1*) The CSA makes a NID for TOP SECRET or SAP information to which the entity requires access. Contractors should be aware that DOE Order 470.4B provides additional information and requirements for processing NID requests for access to RD.

(*2*) In cases in which any category of the proscribed information is controlled by another agency (ODNI for SCI, DOE for RD, the National Security Agency (NSA) for COMSEC), the CSA asks that controlling agency to concur or non-concur on the NID for that category of information.

(*3*) The CSA informs the GCA and the entity when the NID is complete. In cases involving SCI, RD, or COMSEC, the CSA also informs the GCA and the entity when a controlling agency concurs or non-concurs on that agency's category of proscribed information. The entity may begin accessing a category of proscribed information once the CSA informs the GCA and the entity that the controlling agency concurs, even if other categories of proscribed information are pending concurrence.

(*4*) An entity's access to SCI, RD, or COMSEC remains in effect so long as the entity remains eligible for access to classified information and the contract or agreement (or program or project) which imposes the requirement for access to those categories of proscribed information remains in effect, except under any of the following circumstances:

(*i*) The CSA, GCA, or controlling agency becomes aware of adverse information that impacts the entity eligibility determination.

(*ii*) The CSA's threat assessment pertaining to the entity indicates a risk to one of the categories of proscribed information.

(*iii*) The CSA becomes aware of any material change regarding the source, nature, and extent of FOCI.

(*iv*) The entity's record of NISP compliance, based on CSA reviews, becomes less than satisfactory. Consult DOE Order 470.4B for additional information and requirements for processing NID requests for access to RD.

(*5*) Under any of the circumstances in paragraphs (d)(2)(iii)(B)(*4*)(*i*) through (d)(2)(iii)(B)(*4*)(*iv*) in this section, the CSA determines whether the entity remains eligible for access to classified information, it must change the FOCI mitigation measure in order to remain eligible for access to classified information, or the CSA must terminate or revoke the access to classified information.

(*6*) When an entity is eligible for access to classified information that includes a favorable NID for SCI, RD, or COMSEC, the CSA does not have to request a new NID concurrence for the same entity if the access to classified information requirements for the relevant category of proscribed information and terms remain unchanged for:

(*i*) Renewing the contract or agreement.

(*ii*) New task orders issued under the contract or agreement.

(*iii*) A new contract or agreement that contains the same provisions as the previous one (this usually applies when the contract or agreement is for a program or project.)

(*iv*) Renewing the SSA.

(*7*) Under certain conditions, entities under an SSA may not require a NID for one or more categories of proscribed information in accordance with CSA-provided guidance. Categories of proscribed information for entities under SSAs not requiring a NID will be recorded in the CSA's system of record for entity eligibility determinations.

(iv) *Voting Trust (VT) or Proxy Agreement (PA).* The VT and the PA are arrangements that vest the voting rights of the foreign-owned stock in cleared U.S. citizens approved by the USG. Under a VT, the foreign owner transfers legal title its ownership interests in the entity to the trustees. Under a PA, the foreign owner's voting rights are

conveyed to the proxy holders. Neither arrangement imposes any restrictions on the entity's eligibility to have access to classified information or to compete for classified contracts.

(A) Establishment of a VT or PA involves the selection of trustees or proxy holders, all of whom must become members of the entity's governing board. Both arrangements must provide for the exercise of all prerogatives of ownership by the trustees or proxy holders with complete freedom to act independently from the foreign owners, except as provided in the VT or PA. The arrangements may limit the authority of the trustees or proxy holders by requiring approval be obtained from the foreign owner with respect to issues such as:

(*1*) The sale or disposal of the entity's assets or a substantial part thereof.

(*2*) Pledges, mortgages, or other encumbrances on the entity's assets, capital stock, or ownership interests.

(*3*) Mergers, consolidations, or reorganizations.

(*4*) Dissolution.

(*5*) Filing of a bankruptcy petition.

(B) The trustees or proxy holders may consult with the foreign owner, or vice versa, where otherwise consistent with U.S. laws, regulations, and the terms of the VT or PA.

(C) The trustees or proxy holders assume full responsibility for the foreign owner's voting interests and for exercising all governance and management prerogatives relating thereto to ensure the foreign owner will be insulated from the entity, thereby solely retaining the status of a beneficiary. The entity must be organized, structured, and financed to be capable of operating as a viable business entity and independent from the foreign owners' interests that required FOCI mitigation or negation.

(v) *Combination measures.* The CSA may apply combinations of the measures in paragraphs (d)(2)(i) through (d)(2)(iv) in this section or other similar measures that effectively mitigate or negate the risks involved with foreign ownership.

(e) *Limited entity eligibility determination due to FOCI.* In accordance with the provisions of this section and CSA-provided guidance, a limited entity eligibility determination may be an option for a single, narrowly defined contract, agreement, or circumstance for entities under FOCI without mitigation or negation. Limitations on access to classified information are inherent with the granting of limited entity eligibility determinations and are imposed upon all of the entity's employees regardless of citizenship.

(1) In exceptional circumstances, when an entity is under FOCI, the CSA may decide that a limited entity eligibility determination is appropriate when the entity is unable or unwilling to implement FOCI mitigation or negation measures, and the conditions in paragraphs (e)(1)(i) through (iii) of this section are met. This is not the same as a limited entity eligibility determination for purposes not related to FOCI. Information on limited entity eligibility determinations for purposes other than FOCI can be found in § 117.9(m). A CSA may decide that a limited entity eligibility is appropriate for an entity under FOCI if:

(i) The limited entity eligibility determination is in accordance with national security interests and a GCA has informed the CSA that access to classified information by the contractor is essential to contract or agreement performance.

(ii) There is an industrial security agreement with the foreign government of the country from which the FOCI is derived.

(iii) The contractor meets all other entity eligibility requirements outlined in § 117.9(c) except that KMP, other than the FSO, may be citizens of the country from which the FOCI derives and the United States has obtained security assurances at the appropriate level from that country.

(2) A U.S. subsidiary of a foreign entity may be sponsored for a limited entity eligibility determination by a foreign government when the foreign government desires to award a contract or agreement to the U.S. subsidiary that involves access to only that classified information for which the foreign government is the OCA.

(3) Limited entity eligibility determinations are specific to the classified information for the requesting GCA or foreign government and the single narrowly defined contract, agreement, or circumstance the request was based on. The limited entity eligibility determination will only be verified to that GCA or foreign government for the authorized level of access to classified information and any limitations to that access to classified information.

(4) A limited entity eligibility determination is not an option for contractors that require access to proscribed information when a foreign government has ownership or control over the entity.

(5) Release of classified information must be in conformity with the U.S. National Disclosure Policy-1 (provided to designated disclosure authorities on a need-to-know basis from the Office of the Under Secretary of Defense for Policy, Defense Technology Security Administration).

(6) A limited entity eligibility determination will be administratively terminated when there is no longer a need for the contractor to access the classified information for which it was sponsored. Administrative termination of one limited entity eligibility determination does not impact a contractor's other limited entity eligibility determinations.

(7) If there is no industrial security agreement with the foreign government of the country from which the FOCI is derived, in extraordinary circumstances, a limited entity eligibility determination may also be granted if there is a compelling need to do so consistent with U.S. national security interests and the GCA has informed the applicable CSA that access to classified information by the contractor is essential to contract or agreement performance. Under this circumstance, the entity must follow all provisions of this rule.

(f) *Qualifications of trustees, proxy holders, and outside directors.* Individuals who serve as trustees, proxy holders, or outside directors must meet the following criteria:

(1) Trustees and proxy holders must be resident U.S. citizens who can exercise governance and management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the entity.

(2) Outside directors must be resident U.S. citizens who can exercise governance and management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively separated from the entity's classified work.

(3) New trustees, proxy holders, and outside directors must be completely disinterested individuals with no prior involvement with the entity, the entities with which it is affiliated, or the foreign owner.

(4) The CSA may consider other circumstances that may affect an individual's eligibility to serve effectively including the number of boards on which the individual serves, the length of time serving on any other governance boards, and other factors in accordance with CSA-provided guidance.

(5) Trustees, proxy holders, and outside directors must be determined eligible for access to classified information at the level of the entity eligibility determination for access to

classified information. Individuals who are serving as trustees, proxy holders, or outside directors as part of a mitigation measure for the entity are not considered to have prior involvement solely by performing that role for purposes of paragraph (f)(3) of this section.

(g) *Government security committee (GSC).* Under a VT, PA, SSA, or SCA, the contractor is required to establish a permanent committee of its board of directors, known as the GSC.

(1) Unless otherwise approved by the CSA, the GSC consists of trustees, proxy holders, or outside directors and those officer directors who have been determined to be eligible for access to classified information.

(2) The members of the GSC are required to ensure that the contractor adheres to laws and regulations and maintains internal entity policies and procedures to safeguard classified information entrusted to it. The GSC ensures that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

(3) The contractor's FSO will be the principal advisor to the GSC and attend GSC meetings. The chairman of the GSC must concur with the appointment and replacement of FSOs selected by management. The FSO functions will be carried out under the authority of the GSC.

(h) *Additional procedures for FOCI mitigation or negation measures.* In addition to the basic requirements of the FOCI mitigation or negation agreement, the entity may be required to document and implement additional procedures based upon the circumstances of an entity's operations. Those additional procedures will be established in supplements to the FOCI mitigation agreement to allow for flexibility as circumstances change without having to renegotiate the entire agreement. When making use of supplements, the CSA does not consider the FOCI mitigation measure final until the CSA has approved the required supplements. These supplements may include:

(1) *Technology control plan (TCP).* A TCP approved by the CSA will be developed and implemented by those entities cleared under a VT, PA, SSA and SCA and when otherwise deemed appropriate by the CSA. The TCP will prescribe all security measures determined necessary to reasonably prevent the possibility of access by non-U.S. citizen employees and visitors to information for which they are not authorized. The TCP will also prescribe measures designed to assure that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate USG disclosure authorization has been obtained, *e.g.,* an approved export license or technical assistance agreement. Unique badging, escort, segregated work area, security indoctrination schemes, and other measures will be included, as appropriate.

(2) *Electronic communications plan (ECP).* The contractor will develop and implement an ECP, subject to CSA approval, tailored to the contractor's operations to verify that electronic controls are in place for clear technical and logical separation of electronic communications and networks between the contractor, the foreign interest, and its affiliates. The purpose is to prevent the unauthorized disclosure of classified information to the foreign parent or its affiliates. The contractor will include in the ECP a detailed network description and configuration diagram that clearly delineates which networks will be shared and which will be protected from access by the foreign parent or its affiliates. The network description will address firewalls, remote administration, monitoring, maintenance, and separate email servers, as appropriate.

(3) *Affiliated operations plan.* There may be circumstances when the parties to a transaction propose in the FOCI action plan that the U.S. contractor provides certain services for the foreign interest or enters into arrangements with the foreign interest, or the foreign interest provides services for or enters into arrangements with the U.S. contractor. In such circumstances, the contractor will document a plan, subject to CSA approval, outlining the entity's consolidated policies and procedures regarding the control of affiliated operations, regardless of whether such endeavors are administrative, operational, or commercial, performed directly or through third-party service providers, within the entity, or among any of the entity's controlled entities, or the foreign interest and its affiliates.

(4) *Facilities location plan.* When a contractor is potentially collocated with or in close proximity to its foreign parent or an affiliate, the contractor will prepare a facilities location plan to assist the CSA in determining if the contractor is collocated or if the close proximity can be allowed under the FOCI mitigation plan. A U.S. entity generally cannot be collocated with the foreign parent or affiliate, *i.e.,* at the same address or in the same location.

(i) *Annual review and certification.*—(1) *Annual review.* The CSA will meet at least annually, and otherwise as required by circumstances, with the GSCs of contractors operating under a VT, PA, SSA, or SCA to review the purpose and effectiveness of the clearance arrangement and to establish a common understanding of the operating requirements and their implementation. These reviews will include an examination of:

(i) Acts of compliance or noncompliance with the approved security arrangement, standard rules, and applicable laws and regulations.

(ii) Problems or impediments associated with the practical application or utility of the security arrangement.

(iii) Whether security controls, practices, or procedures warrant adjustment.

(2) *Annual certification.* For contractors operating under a VT, PA, SSA, or SCA, the chairman of the GSC will submit to the CSA one year from the effective date of the agreement and annually thereafter, an implementation and compliance report. Such reports will include:

(i) A detailed description of the manner in which the contractor is carrying out its obligations under the agreement.

(ii) Changes to security procedures, implemented or proposed, and the reasons for those changes.

(iii) A detailed description of any acts of noncompliance, whether inadvertent or intentional, with a discussion of remedial measures, including steps taken to prevent such acts from recurring.

(iv) Any changes, or impending changes, of KMP or key board members, including the reasons therefore.

(v) Any changes or impending changes in the organizational structure or ownership, including any reorganizations, acquisitions, mergers, or divestitures.

(vi) Any other issues that could have a bearing on the effectiveness of the applicable agreement.

(j) *Transactions involving foreign persons, and the Committee on Foreign Investment in the United States (CFIUS).*

(1) The CFIUS is a USG interagency committee chaired by the Treasury Department that conducts assessments, reviews and investigations of transactions that could result in foreign control of a U.S. business, and certain non-controlling investments and certain real estate transactions involving foreign persons under 50 U.S.C. 4565.

(2) In CFIUS cases where the acquired U.S. business requires access to classified information, the CFIUS assessment, review or investigation, as applicable, and the CSA industrial

security FOCI review are carried out in parallel, but are separate processes with different time constraints and considerations.

(3) The CSA will promptly advise the parties in a transaction under CFIUS review that would require FOCI negation or mitigation measures if consummated, to submit to the CSA a plan to negate or mitigate FOCI. If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. person that is a party, or in applicable cases, a subject of the proposed transaction fails to comply with the FOCI reporting requirements of this rule, the CSA may recommend a full investigation of the transaction by the CFIUS to determine the effects on national security.

§ 117.12 Security training and briefings.

(a) *General.* Contractors will provide all cleared employees with security training and briefings commensurate with their involvement with classified information.

(b) *Training materials.* Contractors may obtain security, threat awareness, and other education and training information and material from their CSA or other sources.

(c) *Government provided briefings.* The CSA is responsible for providing initial security briefings to the FSO and for ensuring other briefings required for special categories of information are provided to the FSO.

(d) *FSO training.* Contractors will ensure the FSO and others performing security duties complete training considered appropriate by the CSA. Training requirements will be based on the contractor's involvement with classified information. Training may include an FSO orientation course, and for FSOs at contractor locations with a classified information safeguarding capability, an FSO program management course. Contractor FSOs will complete training within six months of appointment to the position of FSO. When determined by the applicable CSA, contractor FSOs must complete an FSO program management course within six months of the CSA approval to store classified information at the contractor.

(e) *Initial security briefings.* Prior to being granted access to classified information, contractors will provide employees with an initial security briefing that includes:

(1) Threat awareness, including insider threat awareness in accordance with paragraph (g) in this section.

(2) Counterintelligence (CI) awareness.

(3) Overview of the information security classification system.

(4) Reporting obligations and requirements, including insider threat.

(5) Cybersecurity training for all authorized information system users in accordance with CSA-provided guidance pursuant to § 117.18(a)(1) and (a)(2).

(6) Security procedures and duties applicable to the employee's position requirements (*e.g.* marking and safeguarding of classified information) and criminal, civil, or administrative consequences that may result from the unauthorized disclosure of classified information, even though the individual has not yet signed an NDA.

(f) *CUI training.* While outside the requirements of the NISPOM, when a classified contract includes provisions for CUI training, contractors will comply with those contract requirements.

(g) *Insider threat training.* The designated ITPSO will ensure that contractor program personnel assigned insider threat program responsibilities and all other cleared employees complete training consistent with applicable CSA provided guidance.

(1) The contractor will provide training to insider threat program personnel, including the contractor's designated ITPSO, on:

(i) CI and security fundamentals.

(ii) Procedures for conducting insider threat response actions.

(iii) Applicable laws and regulations regarding the gathering, integration, retention, safeguarding, and use of records and data, including the consequences of misuse of such information.

(iv) Applicable legal, civil liberties, and privacy policies and requirements applicable to insider threat programs.

(2) The contractor will provide insider threat awareness training to all cleared employees on an annual basis. Depending upon CSA specific guidance, a CSA may instead conduct such training. The contractor must provide all newly cleared employees with insider threat awareness training before granting access to classified information. Training will address current and potential threats in the work and personal environment and will include at a minimum:

(i) The importance of detecting potential insider threats by cleared employees and reporting suspected activity to the insider threat program designee.

(ii) Methodologies of adversaries to recruit trusted insiders and collect classified information, in particular within information systems.

(iii) Indicators of insider threat behavior and procedures to report such behavior.

(iv) CI and security reporting requirements, as applicable.

(3) The contractor will establish procedures to validate all cleared employees who have completed the initial and annual insider threat training.

(h) *Derivative classification.*—(1) *Initial training.* The contractor will ensure all employees authorized to make derivative classification decisions are trained in the proper application of the derivative classification principles, in accordance with CSA direction. Employees are not authorized to conduct derivative classification until they receive such training.

(2) *Refresher training.* In addition to the initial training, contractors will ensure all employees who conduct derivative classification receive training at least once every two years. Contractors will suspend an employee's derivative classification authority for any employee who does not receive such training at least once every two years. Training will emphasize the avoidance of over-classification and address:

(i) Classification levels.

(ii) Duration of classification.

(iii) Identification and markings.

(iv) Classification prohibitions and limitations.

(v) Sanctions and classification challenges.

(vi) Security classification guides.

(vii) Information sharing.

(3) *Record of training.* Contractors will retain records of the date of the most recent training (initial or refresher) and type of training provided to employees.

(i) *Information systems security.* All information system authorized users will receive training on the security risks associated with their user activities and responsibilities under the NISP. The contractor will determine the appropriate content of the training, taking into consideration assigned roles and responsibilities, specific security requirements, and the information system to which personnel are authorized access.

(j) *Temporary help suppliers.* A cleared temporary help supplier, or other contractor who employs cleared individuals solely for dispatch elsewhere, will be responsible for ensuring that required briefings (both initial and refresher training) are provided to their cleared personnel. The temporary help supplier or the using contractor may conduct these briefings.

(k) *Refresher training.* The contractor will provide all cleared employees with security education and training every 12 months. Refresher training will reinforce the information provided during the initial security briefing and will keep cleared employees informed of changes in security regulations and should also address issues or concerns identified during contractor self-reviews. Training methods may include group briefings, interactive videos, dissemination of instructional materials, or other media and methods. Contractors will maintain records about the programs offered and employee participation in them.

(l) *Debriefings.* Contractors will debrief cleared employees and annotate the debriefing in the appropriate contractor records when access to classified information is no longer needed; at the time of termination of employment (discharge, resignation, or retirement); when an employee's eligibility for access to classified information is terminated, suspended, or revoked; and upon termination of the entity eligibility determination.

§ 117.13 Classification.

(a) *Original classification.* Only a USG official designated or delegated the authority in writing can make an original classification decision.

(1) An OCA classifies information pursuant to E.O. 13526 and 32 CFR part 2001, designates and marks it as TOP SECRET, SECRET, or CONFIDENTIAL, and, except as provided by statute, may use no other terms to identify classified information.

(2) The designation UNCLASSIFIED is used to identify information that does not meet the criteria for classification in accordance with E.O. 13526. In accordance with 32 CFR 2002, CUI implementing guidance (including the Marking Handbook) and any GCA-provided guidance, CUI commingled with classified information must be marked as CUI to alert users to its presence and sensitivity. The CUI regulation, guidance, and handbook are available at: *https://www.archives.gov/cui.*

(b) *Derivative classification.* (1) Contractor personnel make derivative classification decisions when they incorporate, paraphrase, restate, or generate in new form, information that is already classified. They must mark the newly developed material consistently with the classification markings that apply to the source information.

(2) Derivative classification is the classification of information based on guidance from an OCA, which may be either a properly marked source document or a current security classification guide provided by a GCA in accordance with E.O. 13526. The duplication or reproduction of existing classified information is not derivative classification.

(3) A source document that does not contain portion markings, due to an ISOO-approved waiver, must contain a warning statement that it may not be used as a source for derivative classification in accordance with 32 CFR 2001.24(k)(4).

(4) Classified information in email messages is marked pursuant to E.O. 13526 and 32 CFR part 2001. If an email is transmitted on a classified system, includes a classified attachment, and contains no classified information within the body of the email itself, the email serves as a transmittal document and is not a derivatively classified document. The email's overall classification must reflect the highest classification level present in the attachment.

(c) *Derivative classification responsibilities.* Contractors will provide employees with pertinent classification guidance to fulfill their derivative classification responsibilities. All contractor employees authorized to make derivative classification decisions will:

(1) Mark the face of each derivatively classified document with a classification authority block that includes the employee's name and position or personal identifier, the entity name, and when applicable, the division or the branch.

FIGURE 1 TO PARAGRAPH (c)(1) EXAMPLE OF INDUSTRY CLASSIFICATION AUTHORITY BLOCK

UNCLASSIFIED: CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Classified by: John Doe, Security Specialist, Entity ABC Security Division
Derived From: SecDef Memo, dtd 20101024, Subj: _____
Declassify On: 20201024

(2) Observe and respect original classification decisions.

(3) Carry forward the pertinent classification markings to any newly created documents. For information derivatively classified based on multiple sources, the derivative classifier will carry forward:

(i) The date or event for declassification that corresponds to the longest period of classification among the sources.

(ii) A listing of the source materials.

(4) Be trained, in accordance with § 117.12(h), in the proper application of the derivative classification principles at least once every two years.

(5) Whenever possible, use a classified addendum if classified information constitutes a small portion of an otherwise unclassified document.

(d) *Security classification guidance.* (1) Contractors should be aware the GCA will:

(i) Incorporate appropriate security requirement clauses in a classified contract, IFB, RFP, RFQ, or all solicitations leading to a classified contract.

(ii) Provide the contractor with the security classification guidance needed during performance of the contract.

(iii) Provide this guidance to the contractor in the contract security classification specification, or equivalent.

(2) The contract security classification specification, or equivalent, must identify the specific elements of classified information involved in the contract that require security protection.

(3) At the discretion of the CSA, contractors may, to the extent possible, advise and assist in the development and any updates to or any revisions to the contract security classification specification, or equivalent.

(4) The contractor will comply with all aspects of the classification guidance.

(i) Users of classification guides are encouraged to notify the originator of the guide when they acquire information that suggests the need for change in the instructions contained in the guide.

(ii) Classification guidance is the exclusive responsibility of the GCA, and the final determination of the appropriate classification for the information rests with that activity. The contract security classification specification, or equivalent, is a contractual specification necessary for the performance of a classified contract. Challenges to classification status are in paragraph (e) in this section.

(iii) If the contractor receives a classified contract without a contract security classification specification, or equivalent, the contractor will notify the GCA. If the GCA does not respond with the appropriate contract security classification specification, or equivalent, the contractor will notify the CSA.

(5) Upon completion of a classified contract, the contractor must return all USG provided or deliverable information to the custody of the USG.

(i) If the GCA does not advise to the contrary, the contractor may retain

copies of the USG material for a period of two years following the completion of the contract. The contract security classification specification, or equivalent, will continue in effect for this two-year period.

(ii) If the GCA determines the contractor has a continuing need for the copies of the USG material beyond the two-year period, the GCA will issue a final contract security classification specification, or equivalent, for the classified contract and will include disposition instructions for the copies.

(e) *Challenges to classification status.* (1) The contractor will address challenges to classification status with the GCA and request remedy when:

(i) Information is classified improperly or unnecessarily.

(ii) Current security considerations justify downgrading to a lower classification level or upgrading to a higher classification level.

(iii) Security classification guidance is not provided, improper or inadequate.

(2) If the GCA does not provide a remedy, and the contractor still believes that corrective action is required, the contractor will make a formal written challenge to the GCA. The challenge will include:

(i) A description sufficient to identify the issue.

(ii) The reasons why the contractor thinks that corrective action is required.

(iii) Recommendations for appropriate corrective action.

(3) The contractor will safeguard the information as required for its assigned or proposed level of classification, whichever is higher, until action is completed.

(4) If the contractor does not receive a written answer from the GCA within 60 days, the contractor will request assistance from the CSA. If the contractor does not receive a response from the GCA within 120 days, the contractor may appeal the challenge to the Interagency Security Classification Appeals Panel through ISOO.

(5) The fact that a contractor has initiated such a challenge will not, in any way, serve as a basis for adverse action against the contractor by the USG. If a contractor believes that adverse action did result from a classification challenge, the contractor will promptly furnish full details to ISOO for resolution.

(f) *Contractor developed information.* Whenever a contractor develops an unsolicited proposal or originates information not in the performance of a classified contract, the provisions of this paragraph apply.

(1) If the information was previously identified as classified, it will be classified according to an appropriate classification guide, or source document, and appropriately marked.

(2) If the information was not previously classified, but the contractor believes the information may or should be classified, the contractor will:

(i) Protect the information as though classified at the appropriate level.

(ii) Submit the information to the agency that has an interest for a classification determination. In such cases, clearly mark the material ''CLASSIFICATION DETERMINATION PENDING; Protect as either TOP SECRET, SECRET, or CONFIDENTIAL.'' This marking will appear conspicuously at least once on the material but no further markings are necessary until a classification determination is received.

(iii) Not be precluded from marking such material as entity-private or entity-proprietary information, unless the material was based upon information obtained from prior deliverables to the USG or was developed from USG material.

(iv) Protect the information pending a final classification determination. The information may be CUI, if it is not classified. Only information that is owned by, produced by, produced for, or is under the control of the USG can be classified in accordance with E.O. 13526.

(3) To be eligible for classification:

(i) The information must incorporate classified information to which the contractor was given prior access.

(ii) The information must be partially or wholly owned by, produced by or for, or under the control of the USG.

(4) 10 CFR 1045.21 includes provisions for the DOE with regard to privately generated RD, whereby the DOE may classify such information in accordance with the AEA.

(g) *Improperly released classified information appearing in public media.* Improperly released classified information is not automatically declassified. When classified information has been improperly released, and even when that classified information has become publicly available, contractors will:

(1) Continue to protect the information at the appropriate classification level until formally advised to the contrary by the GCA.

(2) Bring any questions about the propriety of continued classification in these cases to the immediate attention of the GCA.

(3) Notify the applicable CSA if an employee downloads the improperly released classified information to determine how to resolve a data spill.

(h) *Downgrading or declassifying classified information.* Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. Downgrading or declassifying actions constitute implementation of a directed action based on a review by either the OCA or the USG-designated classification authority. Declassification is not an approval for public disclosure.

(1) *Downgrading.* Contractors will refer information for classification or downgrade to the GCA based on the guidance provided in a contract security classification specification, or equivalent, or upon formal notification.

(2) *Declassification.* Contractors are not authorized to implement downgrading or declassification instructions even when the material is marked for automatic downgrading or declassification. If the material is marked for automatic declassification and the contractor notes that the date or event for the automatic declassification has occurred, the contractor will seek guidance from the GCA.

(i) *RD, FRD, and TFNI.* Protection requirements for RD, FRD, and TFNI are pursuant to § 117.23(e). Information about classification and declassification of RD, FRD, or TFNI documents is in § 117.23(e)(5).

§ 117.14 Marking requirements.

(a) *Purpose for marking.* (1) Physically marking classified information with appropriate classification markings serves to warn and inform holders of the information of the degree of protection required. Other notations facilitate downgrading and declassification, and aid in derivative classification actions.

(2) Contractors will clearly mark all classified information and material to convey to the holder the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, the identity (by name and position or personal identifier) of the classifier, the source(s) for derivative classification, and any other notations required for protection of the information.

(b) *Marking guidance for classified information and material.* Contractors will use the marking guidance conveyed in 32 CFR 2001.22 through 2001.26, and its companion document, ISOO booklet ''Marking Classified National Security Information,'' (available at: *https://www.archives.gov/isoo/training/training-aids*) or CSA specific provided guidance for marking derivatively classified information and material and as required by applicable security

classification guide. The special requirements for marking documents containing RD, FRD, and TFNI are addressed in § 117.23.

(c) *Marking guidance for CUI.* Contractors will use marking guidance conveyed in 32 CFR 2002.20, the CUI Marking Handbook (available at: *https://www.archives.gov/files/cui/documents/20161206-cui-marking-handbook-v1-1-20190524.pdf*), and agency policy to mark CUI in accordance with contract requirements.

(d) *Working papers.* Working papers will be marked, destroyed, and retained in accordance with § 117.15(e)(3).

(e) *Translations.* The contractor will mark translations of U.S. classified information into a language other than English with the appropriate U.S. markings and the foreign language equivalent to show the United States as the country of origin.

(f) *Marking wholly unclassified material.* The contractor will not mark or stamp wholly UNCLASSIFIED material as UNCLASSIFIED unless it is essential to convey to a recipient of such material that:

(1) The material has been examined specifically with a view to impose a security classification and has been determined not to require classification by the GCA.

(2) The material has been reviewed and has been determined to no longer require classification and it has been declassified by the applicable GCA.

(g) *Marking miscellaneous material.* The contractor will:

(1) Handle miscellaneous material developed in connection with the handling, processing, production, storage, and utilization of classified information in a manner that ensures adequate protection of the classified information involved.

(2) Destroy the miscellaneous material at the earliest practical time, unless a requirement exists to retain such material. Notwithstanding the provisions of paragraph (a) of this section, there is no requirement for the contractor to mark such material, but disposition and retention requirements in § 117.15(i) and (j) apply.

(h) *Marking training material.* The contractor will clearly mark unclassified documents or materials that are created to simulate or demonstrate classified documents or material to indicate the actual UNCLASSIFIED status of the information. For example, the contractor may use: MARKINGS ARE FOR TRAINING PURPOSES ONLY, OTHERWISE UNCLASSIFIED or UNCLASSIFIED SAMPLE, or other similar marking.

(i) *Downgrading or declassification actions.* When a contractor removes documents or material that have been downgraded or declassified from storage for use or for transmittal outside the contractor location:

(1) The documents or material must be re-marked pursuant to paragraph (i)(1)(i) or (i)(1)(ii) in this section.

(i) Prior to taking any action to downgrade or declassify information, the contractor will seek guidance from the GCA. If the GCA approves such action, the contractor will cancel all old classification markings with the new markings substituted, whenever practical. For documents, at a minimum the outside of the front cover, the title page, the first page, and the outside of the back will reflect the new classification markings, or include the designation UNCLASSIFIED. The contractor will re-mark other material by the most practical method for the type of material involved to ensure that it is clear to the holder what level of classification is assigned to the material.

(ii) When the GCA notifies contractors of downgrading or declassification actions that are contrary to the markings shown on the material, the contractor will re-mark material to indicate the change and notify other holders if further dissemination was made. The contractor will mark the material to indicate the:

(A) Authority for the action.

(B) Date of the action.

(C) Identity and position of the individual taking the action.

(2) If the volume of material is such that prompt re-marking of each classified item cannot be accomplished without unduly interfering with operations, the contractor may attach a downgrading and declassification notice to the inside of the file drawers or other storage container instead of the re-marking otherwise required.

(3) When such documents or materials are withdrawn from the container solely for transfer to another container, or when the container is transferred from one place to another, the transfer may be made without re-marking if the notice is attached to the new container or remains with each shipment.

(4) For the purpose of paragraphs (i)(2) and (i)(3) in this section, the contractor must include in the downgrading and declassification notice:

(i) The authority for the downgrading or declassification action.

(ii) The date of the action.

(iii) The storage container to which it applies.

(j) *Upgrading action.* (1) When the contractor receives notice from the GCA to upgrade material to a higher level; for example, from CONFIDENTIAL to SECRET, the contractor will:

(i) Immediately enter the new markings on the material according to the notice to upgrade, and strike through all the superseded markings.

(ii) Enter the authority for and the date of the upgrading action on the material.

(iii) Ensure all records affected are stored at the appropriate level of security, including digital networks and systems. Upgrades requiring network or system adjustment will be coordinated with the GCA to mitigate or account for impact on the execution of the contract.

(2) The contractor will notify all holders to whom they disseminated the material. The contractor will not mark the notice as classified unless it contains additional information warranting classification.

(3) In the case of material which was inadvertently released as UNCLASSIFIED, the contractor will mark and protect the notice as classified at the CONFIDENTIAL level, unless it contains additional information warranting a higher classification. The contractor will cite the applicable Contract Security Classification Specification, or equivalent, or other classification guide on the ''Derived From'' line and mark the notice with an appropriate declassification instruction.

(k) *Dissemination of improperly marked information.* If the contractor inadvertently distributes classified material without the proper classification assigned to it, or without any markings to identify the material as classified, as appropriate, the contractor will:

(1) Determine whether all holders of the material are cleared and authorized access to it.

(2) If recipients are authorized persons, and the contractor disseminated the information through authorized channels, promptly provide written notice to all holders of the proper classification to be assigned. The contractor will also include the classification source as well as declassification instructions in the notification.

(3) Report compromises to the CSA in accordance with the provisions of § 117.8(d), if:

(i) Any of the recipients of the material are not authorized persons.

(ii) Any material cannot be accounted for.

(iii) The material was transmitted through unauthorized channels.

(l) *Marking foreign government classified material.* Foreign government classified information will retain its original classification markings or will be assigned a U.S. classification that provides a degree of protection at least equivalent to that required by the foreign government entity that furnished the information in accordance with 32 CFR 2001.54. The equivalent U.S. classification and the country of origin will be marked on the front and back in English.

(m) *Foreign government restricted information and ''in confidence'' information.*

(1) Some foreign governments have a fourth level of classification that does not correspond to an equivalent U.S. classification that is identified as RESTRICTED information. In many cases, security agreements require RESTRICTED information to be protected as U.S. CONFIDENTIAL information.

(2) Some foreign governments may have a category of unclassified information that is protected by law. This latter category is normally provided to other governments with the expectation that the information will be treated ''In Confidence.'' The foreign government or international organization must state that the information is provided in confidence and that it must be protected from release.

(i) 10 U.S.C. 130c protects information provided ''In Confidence'' by foreign governments which is not classified but meets special requirements.

(ii) This provision also applies to RESTRICTED information which is not required by an agreement to be protected as classified information.

(iii) The contractor will not disclose information protected by this statutory provision to anyone except personnel who require access to the information in connection with the contract.

(3) It is the responsibility of the foreign entity that awards the contract to incorporate requirements for the protection and marking of RESTRICTED or ''In Confidence'' information in the contract. The contractor will advise the CSA if requirements were not provided by the foreign entity.

(n) *Marking U.S. documents containing FGI.* (1) U.S. documents containing FGI must be marked on the front, ''THIS DOCUMENT CONTAINS (indicate country of origin) INFORMATION.'' In addition, the portions must be marked to identify both the country and classification level, (*e.g.,* (UK–C), (GE–C)). The ''Derived From'' line will identify U.S. as well as foreign classification sources.

(2) If the identity of the foreign government must be concealed, the front of the document will be marked ''THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT INFORMATION;'' paragraphs will be marked FGI, together with the classification level (*e.g.,* (FGI–C)); and the ''Derived From'' line will indicate FGI in addition to any U.S. source. The identity of the foreign government will be maintained with the record copy of the document.

(3) A U.S. document that contains FGI will not be downgraded below the highest level of FGI contained in the document or be declassified without the written approval of the foreign government that originated the information. Recommendations concerning downgrading or declassification will be submitted to the GCA or foreign government contracting authority, as applicable.

(o) *Marking documents prepared for foreign governments.* Documents prepared for foreign governments that contain U.S. classified information and FGI will be marked as prescribed by the foreign government. In addition, they will be marked on the front, ''THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION.'' Portions will be marked to identify the U.S. classified information.

(p) *Marking requirements for transfers of defense articles to Australia (AUS) or the United Kingdom (UK).* Marking requirements for transfers of defense articles to AUS or the UK without a license or other written authorization are pursuant to § 117.19(i).

(q) *Commingling of RD and FRD.* Commingling of RD, FRD, and TFNI with national security information (NSI) in the same document should be avoided to the greatest degree possible. When mixing this information cannot be avoided, the marking requirements in 10 CFR part 1045, section 140(f) and declassification requirements of 10 CFR part 1045, section 155 apply.

§ 117.15 Safeguarding Classified Information.

(a) *General safeguarding.* Contractors will be responsible for safeguarding classified information in their custody or under their control, with approval for such storage of classified information by the applicable CSA. Individuals are responsible for safeguarding classified information entrusted to them. Contractors will provide the extent of protection to classified information sufficient to reasonably protect it from loss or compromise.

(1) *Oral discussions.* Contractors will ensure that all cleared personnel are aware of the prohibition against discussing classified information over unsecured telephones, in public conveyances or places, or in any other manner that permits interception by unauthorized persons.

(2) *End of day security checks.* (i) Contractors that store classified material will establish a system of security checks at the close of each working day to verify that all classified material and security repositories have been appropriately secured.

(ii) Contractors that operate multiple work shifts will perform the security checks at the end of the last working shift in which classified material was removed from storage for use. The checks are not required during continuous 24-hour operations.

(3) *Perimeter controls.* (i) Contractors authorized to store classified material will establish and maintain a system to deter and detect unauthorized introduction or removal of classified material from their facility without proper authority.

(ii) If the unauthorized introduction or removal of classified material can be reasonably prevented through technical means (*e.g.,* an intrusion detection system), which are encouraged, no further controls are necessary. The contractor will provide appropriate authorization to personnel who have a legitimate need to remove or transport classified material for passing through designated entry or exit points.

(iii) The contractor will:

(A) Provide appropriate authorization to personnel who have a legitimate need to remove or transport classified material for passing through designated entry or exit points.

(B) Conspicuously post notices at all pertinent entries and exits that persons who enter or depart the facility are subject to an inspection of their personal, except under circumstances where the possibility of access to classified material is remote.

(C) Limit inspections to buildings or areas where classified work is being performed.

(D) Establish the extent, frequency, and location of inspections in a manner consistent with contractual obligations and operational efficiency. The contractor may use any appropriate random sampling technique.

(E) Seek legal advice during the formulation of implementing procedures.

(F) Submit significant problems pertaining to perimeter controls and inspections to the CSA.

(iv) Contractors will develop procedures for safeguarding classified material in emergency situations.

(A) The procedures should be as simple and practical as possible and adaptable to any type of emergency that may reasonably arise.

(B) Contractors will promptly report to the CSA any emergency situation that renders them incapable of safeguarding classified material.

(b) *Standards for Security Equipment.* Contractors will follow guidelines established in 32 CFR part 2001, when procuring storage and destruction equipment. Authorized repairs for GSA-approved security containers and vaults must be in accordance with Federal Standard 809.

(c) *Storage.* Contractors will store classified information and material in General Services Administration (GSA)-approved security containers, vaults built to Federal Standard 832, or an open storage area constructed in accordance with 32 CFR 2001.53. In the instance that an open storage area has a false ceiling or raised floor, contractors shall develop and implement procedures to ensure their structural integrity. Nothing in 32 CFR part 2001, should be construed to contradict or inhibit compliance with local laws or building codes, but the contractor will notify the applicable CSA if there are any conflicting issues that would inhibit compliance. Contractors will store classified material in accordance with the specific sections of 32 CFR 2001.43:

(1) CONFIDENTIAL. See 32 CFR 2001.43(b)(3).

(2) SECRET. See 32 CFR 2001.43(b)(2).

(3) TOP SECRET Documents. See 32 CFR 2001.43(b)(1).

(d) *Intrusion Detection Systems (IDS).* This paragraph specifies the minimum standards for an approved IDS when used for supplemental protection of TOP SECRET and SECRET material. The CSA will provide additional guidance for contingency protection procedures in the event of IDS malfunction, including contractors located in USG owned contractor operated facilities.

(1) *CSA approval.* (i) CSA approval is required before installing an IDS. The CSA will base approval of a new IDS on the criteria of Intelligence Community Directive 705 (available at: *https://www.dni.gov/files/documents/ICD/ICD_705_SCIFs.pdf*) and any applicable intelligence community standard, Underwriters Laboratories (UL) Standard 2050 (Government agencies with a role as a CSA or CSO may obtain this reference without charge; available at: *www.ul.com/contact*), or the CSA may base approval on written CSA-specific standards for the information to be protected.

(ii) Installation will be performed by an alarm services company certified by a NRTL that meets the requirements in 29 CFR 1910.7 to perform testing and certification. The NRTL-approved alarm service company is responsible for completing the appropriate alarm system description form approved by the NRTL.

(iii) All the intrusion detection equipment (IDE) used in the IDS installation will be tested and approved (or listed) by a NRTL, ensuring its proper operation and resistance from tampering. Any IDE that has not been tested and approved by a NRTL will require CSA approval.

(2) *Central monitoring station.* (i) For the purpose of monitoring alarms, an equivalent level of monitoring service is available from multiple types of providers. The central monitoring station may be located at a one of the following:

(A) Government contractor monitoring station (GCMS), formerly called a proprietary central station.

(B) Cleared commercial central station.

(C) Cleared protective signal service station (*e.g.,* fire alarm monitor).

(D) Cleared residential monitoring station.

(E) National industrial monitoring station.

(ii) SECRET-cleared central station employees at the alarm monitoring station will be in attendance in sufficient number to monitor each alarmed area within the cleared contractor facility.

(iii) The central monitoring station will be supervised continuously by a U.S. citizen who has eligibility for access to SECRET information.

(iv) The IDS must be activated at the close of business whenever the area is not occupied by cleared personnel. Any IDS exit delay function must expire prior to the cleared personnel leaving the immediate area. A record will be maintained to identify the person or persons who are responsible for setting and deactivating the IDS.

(v) Records will be maintained for 12 months indicating time of receipt of alarm, name(s) of security force personnel responding, time dispatched to facility or area, time security force personnel arrived, nature of alarm, and what follow-up actions were accomplished.

(3) *Investigative response to alarms.* (i) Alarm response teams will ascertain if intrusion has occurred and, if possible, assist in the apprehension of the individuals involved.

(A) If an alarm activation resets in a reasonable amount of time and no damage to the area is visible, then entrance into the area is not required and an initial response team may consist of uncleared personnel.

(B) If the alarm activation does not reset and damage is observed, then a cleared response team must be dispatched. The initial uncleared response team must stay on station until relieved by the cleared response team. If a cleared response team does not arrive within 1 hour, then a report to the CSA must be made by the close of the next business day.

(ii) The following resources may be used to investigate alarms: Proprietary security force personnel, central station guards, local law enforcement personnel, or a subcontracted guard service. The CSA may approve procedures for the use of entity cleared employees who can meet the minimum response requirements outlined in this section.

(A) For a GCMS, trained proprietary or subcontractor security force personnel, cleared to the SECRET level and sufficient in number to be dispatched immediately to investigate each alarm, will be available at all times when the IDS is in operation.

(B) For a commercial central station, protective signaling service station, or residential monitoring station, there will be a sufficient number of trained guards available to respond to alarms. Guards will be cleared only if they have the ability and responsibility to access the area or container(s) housing classified material (*i.e.,* keys to the facility have been provided or the personnel are authorized to enter the building or check the container or area that contains classified material).

(C) Uncleared guards dispatched by a commercial central station, protective signaling service station, or residential monitoring station in response to an alarm will remain on the premises until a designated, cleared representative of the facility arrives, or for a period of not less than 1 hour, whichever comes first. If a cleared representative of the facility does not arrive within 1 hour following the arrival of the guard, the central control station must provide the CSA with a report of the incident that includes the name of the subscriber facility, the date and time of the alarm, and the name of the subscriber's representative who was contacted to respond. A report will be submitted to the CSA by the end of business on the next business day.

(D) Subcontracted guards must be under a classified contract with either the installing alarm service company or the cleared facility.

(iii) The response time will be in accordance with the provisions in paragraphs (c)(1) through (c)(3) in this section as applicable. When environmental factors (*e.g.,* traffic, distance) legitimately prevent meeting the requirements for TOP SECRET information, as indicated in paragraph (c)(3) in this section, the CSA may authorize up to a 30-minute response time. The CSA approval will be documented on the alarm system description form and the specified response time will be noted on the alarm certificate. The requirement for response is 80 percent within the time limits.

(4) *Installation.* The IDS will be installed by an NRTL-approved entity or by an entity approved in writing by the CSA. When connected to a commercial central station, GCMS, national industrial monitoring station, or residential monitoring station, the service provided will include line security (*i.e.,* the connecting lines are electronically supervised to detect evidence of tampering or malfunction). The level of protection for the alarmed area will include all points of probable entry (perimeter doors and accessible windows) with magnetic contacts and motion detectors positioned in the probable intruder paths from the probable points of entry to the classified information. In accordance with Federal Standard 809, no IDS sensors (magnetic contacts or vibration detectors) will be installed on GSA-approved security containers. CSA authorization on the alarm system description form is required in the following circumstances:

(i) When line security is not available, installation will require two independent means of transmission of the alarm signal from the alarmed area to the monitoring station.

(ii) Alarm installation provides a level of protection, *e.g.* UL's Extent 5, based on patrolling employees and CSA approval of security-in-depth.

(iii) Where law enforcement personnel are the primary alarm response. Under those circumstances, the contractor must obtain written assurance from the police department regarding the ability to respond to alarms in the required response time.

(iv) Alarm signal transmission is over computer-controlled data-networks (*e.g.,* internet, intranet). The CSA will provide specific acceptance criteria (*e.g.,* encryption requirements) for alarms monitored over data networks.

(v) Alarm investigator response time exceeds the parameters outlined in paragraphs (c)(1) through (c)(3) in this section as applicable.

(5) *Certification of compliance.* Evidence of compliance with the requirements of this section will consist of a valid (current) certification by an approved NRTL for the appropriate category of service. This certificate:

(i) Will have been issued to the protected facility by the NRTL, through the alarm service company.

(ii) Serves as evidence that the alarm service company that did the installation is:

(A) Listed as furnishing security systems of the category indicated.

(B) Authorized to issue the certificate of installation as representation that the equipment is in compliance with requirements established by NRTL for the class of alarm system.

(C) Subject to the NRTL inspection program whereby periodic inspections are made of representative alarm installations by NRTL personnel to verify the correctness of certification practices.

(6) *Exceptional cases.* (i) If the requirements in paragraphs (d)(1) through (d)(5) in this section cannot be met, the contractor may request CSA approval for an alarm system meeting one of these conditions, which will be documented on the alarm system description form:

(A) Monitored by a central control station but responded to by a local (municipal, county, state) law enforcement organization.

(B) Connected by direct wire to alarm receiving equipment located in a local (municipal, county, State) police station or public emergency service dispatch center. This alarm system is activated and deactivated by employees of the contractor, but the alarm is monitored and responded to by personnel of the monitoring police or emergency service dispatch organization. Personnel monitoring alarm signals at police stations or dispatch centers do not require PCLs. Police department response systems may be requested only when:

(*1*) The contractor facility is located in an area where central control station services are not available with line security or proprietary security force personnel, or a contractually-dispatched response to an alarm signal cannot be achieved within the time limits required by the CSA.

(*2*) It is impractical for the contractor to establish a GCMS or proprietary guard force at that location. In this case, installation of these systems must use NRTL-approved equipment and be accomplished by an NRTL-approved entity meeting the applicable testing standard for the category of service.

(ii) An installation proposal, explaining how the system would operate, will be submitted to the CSA. The proposal must include:

(A) Sufficient justification for the granting of an exception and the full name and address of the police department that will monitor the system and provide the required response.

(B) The name and address of the NRTL-approved entity that will install the system, and inspect, maintain, and repair the equipment.

(iii) The response times will be in accordance with the provisions in paragraphs (c)(1) through (c)(3) in this section as applicable. Arrangements will be made with the central monitoring station to immediately notify a contractor representative on receipt of the alarm. The contractor representative is required to go immediately to the facility to investigate the alarm and to take appropriate measures to secure the classified material.

(iv) In exceptional cases where central station monitoring service is available, but no proprietary security force, central station, or subcontracted guard response is available, and where the police department does not agree to respond to alarms, and no other manner of investigative response is available, the CSA may approve cleared employees as the sole means of response.

(e) *Information controls.*—(1) *Information management system.* Contractors will establish:

(i) A system to verify that classified information in their custody is used or retained only for a lawful and authorized USG purpose.

(ii) An information management system to protect and control the classified information in their possession regardless of media, to include information processed and stored on authorized information systems.

(2) *Top secret information.* Contractors will establish controls for TOP SECRET information and material to validate procedures are in place to address accountability, need to know, and retention, e.g., demonstrating that TOP SECRET material stored in an electronic format on an authorized classified information system does not need to be individually numbered in series. These controls are in addition to the information management system and must be applied, unless otherwise directed by the applicable CSA, regardless of the media of the TOP SECRET information, to include information processed and stored on authorized information systems. Unless otherwise directed by the applicable

CSA, the contractor will establish the following additional controls:

(i) Designate TOP SECRET control officials to receive, transmit, and maintain access and accountability records to TOP SECRET information.

(ii) Conduct an annual inventory of TOP SECRET information and material.

(iii) Establish a continuous receipt system for the transmittal of TOP SECRET information within and outside the contractor location.

(iv) Number each item of TOP SECRET material in a series. Place the copy number on TOP SECRET documents, regardless of media, and on all associated transactions documents.

(v) Establish a record of TOP SECRET material when the material is:

(A) Completed as a finished document.

(B) Retained for more than 180 days after creation, regardless of the stage of development.

(C) Transmitted outside the contractor location.

(vi) Establish procedures for destruction of TOP SECRET material by two authorized persons.

(vii) Establish destruction records for TOP SECRET material and maintain the records for two years in accordance with § 117.13(d)(5) or in accordance with GCA requirements.

(3) *Working papers.* Contractors will establish procedures for the control of classified working papers generated in the preparation of a finished document. The contractor will:

(i) Date working papers when they are created.

(ii) Mark each page of the working papers with the highest classification level of any information contained in them and with the annotation ''WORKING PAPERS.''

(iii) Destroy working papers when no longer needed.

(iv) Mark in the same manner prescribed for a finished document at the same classification level if released outside the contractor location or retained for more than 180 days from the date of origin.

(4) *Combinations to locks.* Contractors will follow the guidance in 32 CFR 2001.45(a)(1) and 2001.43 (c) to address thresholds when combinations will be changed. Combinations to locks used to secure vaults, open storage areas, and security containers that are approved for the safeguarding of classified information will be protected in the same manner as the highest level of classified information that the vault, open storage area, or security container is used to protect.

(5) *Information system passwords.* Contractors will follow the guidance established in 32 CFR 2001.45(a)(2) for the protection of passwords to information systems authorized to process and store classified information at the highest level of classification to which the information system is authorized.

(6) *Reproduction of classified information.* Contractors will follow the guidance established in 32 CFR 2001.45(b) for the reproduction of classified information.

(f) *Transmission of classified information.* Contractors will establish procedures for transmitting and receiving classified information and material in accordance with 32 CFR 2001.46.

(1) *Top secret.* The contractor must have written authorization from the GCA to transmit TOP SECRET material outside the contractor location.

(2) *Transmission outside the United States and its Territorial Areas.* The contractor may transmit classified material to a USG activity outside the United States or a U.S. territorial area only under the provisions of a classified contract or with written authorization from the GCA.

(3) *Commercial delivery entities.* The CSA may approve contractors to transmit SECRET or CONFIDENTIAL information within the United States and its territorial areas by means of a commercial delivery entity that is a current holder of the GSA contract for overnight delivery, and which provides nation-wide, overnight service with computer tracking and reporting features (a list of current contract holders may be found at: *https://www.archives.gov/isoo/faqs#what-is-overnightcarriers*). Such entities do not need to be determined eligible for access to classified information.

(i) Prior to CSA approval, the contractor must establish and document procedures to ensure the proper protection of incoming and outgoing classified packages, including the street delivery address, for each cleared facility intending to use GSA-listed commercial delivery entities for overnight services.

(ii) Contractors will establish procedures for the use of commercial delivery entities in accordance with 32 CFR part 2001. The procedures will:

(A) Confirm that the commercial delivery entity provides nationwide, overnight delivery service with automated in-transit tracking of the classified packages.

(B) Ensure the package integrity during transit and that incoming shipments are received by appropriately cleared personnel.

(C) Not be used for COMSEC, NATO, or FGI.

(4) *Couriers and hand carriers.* Contractors may designate cleared employees as couriers or hand carriers. Contractors will:

(i) Brief employees providing such services on their responsibility to safeguard classified information and keep classified material in their possession at all times.

(ii) Provide employees with an identification card or badge which contains the contractor's name and the name and a photograph of the employee.

(iii) Make arrangements in advance of departure for overnight storage at a USG installation or at a cleared contractor's facility that has appropriate storage capability, if needed.

(iv) Conduct an inventory of the material prior to departure and upon return. The employee will carry a copy of the inventory with them.

(5) *Use of commercial passenger aircraft.* The contractor may authorize cleared employees to hand carry classified material aboard commercial passenger aircraft.

(i) *Routine processing.* Employees hand carrying classified material are subject to routine processing by airline security agents. Hand-held packages will normally be screened by x-ray examination. If security personnel are not satisfied with the results of the inspection and requests the prospective passenger to open a classified package for visual examination, the traveler must inform the screener that the carry-on items contain USG classified information and cannot be opened. Under no circumstances may traveler or security personnel open the classified material unless required by customs or other government officials.

(ii) *Special processing.* The contractor will contact the appropriate air carrier in advance to explain the particular circumstances and obtain instructions on the special screening procedures to follow when:

(A) Routine processing would subject the classified material to compromise or damage.

(B) Visual examination is or may be required to successfully screen a classified package.

(C) Classified material is in specialized containers, which due to its size, weight, or other physical characteristics cannot be routinely processed.

(iii) *Authorization letter.* Contractors will provide employees with written authorization to hand carry classified material on commercial aircraft that includes:

(A) Full name, date of birth, height, weight, and signature of the traveler and statement that he or she is authorized to transmit classified material.

(B) Description of the type of identification the traveler will present on request.

(C) Description of the material being hand carried, with a request that it be exempt from opening.

(D) Identification of the points of departure, destination, and known transfer points.

(E) Name, telephone number, and signature of the FSO, and the location and telephone number of the CSA.

(6) *Escorts.* If an escort is necessary to ensure the protection of the classified information being transported, the contractor will assign a sufficient number to each classified shipment to ensure continuous surveillance and control over the shipment while in transit. The contractor will furnish escorts with specific written instructions and operating procedures prior to shipping that include:

(i) Name and address of persons, including alternates, to whom the classified material is to be delivered.

(ii) Receipting procedures.

(iii) Means of transportation and the route to be used.

(iv) Duties of each escort during movement, during stops end route, and during loading and unloading operations.

(v) Emergency and communication procedures.

(g) *Destruction.* Contractors will:

(1) Destroy classified material in their possession based on the disposition instructions in the contract security classification specification or equivalent.

(2) Follow the guidance for destruction of classified material in accordance with 32 CFR 2001.47 and the destruction equipment standards in accordance with 32 CFR 2001.42(b). See *https://www.nsa.gov/resources/everyone/media-destruction/* and any CSA provided guidance for additional information.

(h) *Disclosure.* Contractors will establish processes by which classified information is disclosed only to authorized persons.

(1) *Disclosure to employees.* Contractors are authorized to disclose classified information to their cleared employees with the appropriate eligibility for access to classified information and need to know as necessary, including cleared employees across the MFO, when applicable, for the performance of tasks or services essential to the fulfillment of a classified contract or subcontract.

(2) *Disclosure to subcontractors.*—(i) *Contractors:* (A) Are authorized to disclose classified information to a cleared subcontractor with the appropriate entity eligibility determination (also known as a facility security clearance) and need to know when access to classified information is necessary for the performance of tasks or services essential to the fulfillment of a prime contract or a subcontract.

(B) Will convey appropriate classification guidance for the classified information to be disclosed with the subcontract in accordance with § 117.13.

(ii) *The CSA must have:* (A) Made a determination of eligibility for access to classified information for the subcontractor, at the same level, or higher, than the classified information to be disclosed, to allow for such disclosures.

(B) Approved storage capability for classified material at the subcontractor location if a physical transfer of classified material occurs.

(3) *Disclosure between parent and subsidiaries*—(i) *Contractors:* (A) Are authorized to disclose classified information between parent and subsidiary entities with the appropriate entity eligibility determination (also known as a facility security clearance) and need to know when access to classified information is necessary for the performance of tasks or services essential to the fulfillment of a prime or subcontract.

(B) Will convey appropriate classification guidance with the agreement or procurement action that necessitates the disclosure.

(ii) *The CSA must have:* (A) Made a determination of eligibility for access to classified information for both the parent and subsidiary, at the same level, or higher, than the classified information to be disclosed, to allow for such disclosures.

(B) Approved storage capability for classified material at the parent and the subsidiary if a physical transfer of classified material occurs.

(4) *Disclosure to federal agencies.* Contractors will not disclose classified information received or generated under a contract from one agency to any other federal agency unless specifically authorized by the agency that has classification jurisdiction over the information.

(5) *Disclosure of classified information to foreign persons.* Contractors will not disclose classified information to foreign persons unless specified by the contract and release of the information is authorized in writing by the government agency having classification jurisdiction over the information involved, *i.e.* the DOE for RD and FRD (also see § 117.23), the NSA for COMSEC, the DNI for SCI, and all other executive branch departments and agencies for classified information under their respective jurisdictions.

(6) *Disclosure to other contractors.* Contractors will not disclose classified information to another contractor except in furtherance of a contract, subcontract, or other GCA purpose without the authorization of the GCA, if such authorization is required by contract.

(7) *Disclosure of classified information in connection with litigation.* Contractors will not disclose classified information to:

(i) Attorneys hired solely to represent the contractor in any civil or criminal case in federal or State courts unless the disclosure is specifically authorized by the agency that has jurisdiction over the information.

(ii) Any federal or state court except on specific instructions of the agency, which has jurisdiction over the information or the attorney representing the United States in the case.

(8) *Disclosure to the public.* Contractors will not disclose classified information to the public. Contractors will not disclose unclassified information pertaining to a classified contract to the public without prior review and clearance as specified in the Contract Security Classification Specification, or equivalent, for the contract or as otherwise specified by the GCA. The procedures of this paragraph also apply to information pertaining to classified contracts intended for use in unclassified brochures, promotional sales literature, reports to stockholders, or similar material.

(i) The contractor will:

(A) Submit requests for approval through the activity specified in the GCA-provided classification guidance for the contract involved.

(B) Include in each request the approximate date the contractor intends to release the information for public disclosure and identify the media to be used for the initial release.

(C) Retain a copy of each approved request for release for a period of one inspection cycle for review by the CSA.

(D) Clear all information developed subsequent to the initial approval through the appropriate office prior to public disclosure.

(ii) Unless specifically prohibited by the GCA, the contractor does not need to request approval for disclosure of:

(A) The fact that a contract has been received, including the subject of the contract or type of item in general terms

provided the name or description of the subject is not classified.

(B) The method or type of contract.

(C) Total dollar amount of the contract unless that information equates to:

(*1*) A level of effort in a sensitive research area.

(*2*) Quantities of stocks of certain weapons and equipment that are classified.

(D) Whether the contract will require the hiring or termination of employees.

(E) Other information that from time-to-time may be authorized on a case-by-case basis in a specific agreement with the contractor.

(F) Information previously officially approved for public disclosure.

(iii) Information that has been declassified is not authorized for public disclosure. If the information is comingled with CUI, or qualifies as CUI once declassified, it will be marked and protected as CUI until it is decontrolled pursuant to 32 CFR part 2002 and reviewed for public release. If the information does not qualify as CUI, it will be protected in accordance with the basic safeguarding requirements in 48 CFR 52.204–21 and subject to the agency's public release procedures. Contractors will request approval for public disclosure of declassified information in accordance with the procedures of this paragraph.

(i) *Disposition.* Contractors will:

(1) Establish procedures for review of their classified holdings on a recurring basis to ensure the classified holdings are in support of a current contract or authorization to retain beyond the end of the contract period.

(2) Destroy duplicate copies as soon as practical.

(3) For disposition of classified material not received under a specific contract:

(i) Return or destroy classified material received with a bid, proposal, or quote if the bid, proposal, or quote is not:

(A) Submitted or is withdrawn within 180 days after the opening date of bids, proposals, or quotes.

(B) Accepted within 180 days after notification that a bid, proposal, or quote has not been accepted.

(ii) If the classified material was not received under a specific contract, such as material obtained at classified meetings or from a secondary distribution center, return or destroy the classified material within one year after receipt.

(j) *Retention.* The provisions of § 117.13(d)(5) apply for retention of classified material upon completion of a classified contract.

(1) If contractors propose to retain copies of classified material beyond 2 years, the contractor will identify:

(i) TOP SECRET material identified in a list of specific documents unless the GCA authorizes identification by subject and approximate number of documents.

(ii) SECRET and CONFIDENTIAL material may be identified by general subject and the approximate number of documents.

(iii) Contractors will include a statement of justification for retention beyond two years based on if the material:

(A) Is necessary for the maintenance of the contractor's essential records.

(B) Is patentable or proprietary data to which the contractor has the title.

(C) Will assist the contractor in independent research and development efforts.

(D) Will benefit the USG in the performance of other prospective or existing agency contracts.

(E) Will benefit the USG in the performance of another active contract and will be transferred to that contract (specify contract).

(2) If the GCA does not authorize retention beyond two years, the contractor will destroy all classified material received or generated in the performance of a classified contract unless it has been declassified or the GCA has requested that the material be returned.

(k) *Termination of security agreement.* Notwithstanding the provisions for retention outlined in paragraph (i) in this section, in the event that the CSA terminates the contractor's eligibility for access to classified information, the contractor will return all classified material in its possession to the GCA concerned, or dispose of such material in accordance with instructions from the CSA.

(l) *Safeguarding CUI.* While outside the requirements of the NISPOM, when a classified contract also includes provisions for protection of CUI, contractors will comply with those contract requirements.

§ 117.16 Visits and meetings.

(a) *Visits.* This paragraph applies when, for a lawful and authorized USG purpose, it is anticipated that classified information will be disclosed during a visit to a cleared contractor facility or to a USG facility.

(1) *Classified visits.* The number of classified visits will be held to a minimum. The contractor:

(i) Must determine that the visit is necessary and the purpose of the visit cannot be achieved without access to, or disclosure of, classified information.

(ii) Will establish procedures to ensure positive identification of visitors, appropriate PCL, and need-to-know prior to the disclosure of any classified information.

(iii) Will establish procedures to ensure that visitors are only afforded access to classified information consistent with the purpose of the visit.

(2) *Need-to-know determination.* The responsibility for determining need-to-know in connection with a classified visit rests with the individual who will disclose classified information during the visit. Need-to-know is generally based on a contractual relationship between the contractors. In other circumstances, disclosure of the information will be based on an assessment that the receiving contractor has a bona fide need to access the information in furtherance of a GCA purpose.

(3) *Visits by USG representatives.* Representatives of the USG, when acting in their official capacities as inspectors, investigators, or auditors, may visit a contractor's facility, provided these representatives present appropriate USG credentials upon arrival.

(4) *Visit authorization.* (i) If a visit requires access to classified information, the host contractor will verify the visitor's PCL level. Verification of a visitor's PCL may be accomplished by a review of a CSA-designated database that contains the information or by a visit authorization letter (VAL) provided by the visitor's employer.

(ii) If a CSA-designated database is not available and a VAL is required, contractors will include in all VALs:

(A) Contractor's name, employee's name, address, and telephone number, assigned commercial and government entity (CAGE) code, if applicable, and certification of the level of the entity eligibility determination.

(B) Name, date and place of birth, and citizenship of the employee intending to visit.

(C) Certification of the proposed visitor's PCL and any special access authorizations required for the visit.

(D) Name of person(s) to be visited.

(E) Purpose and sufficient justification for the visit to allow for a determination of the necessity of the visit.

(F) Date or period during which the VAL is to be valid.

(5) *Long term visitors.* (i) When USG employees or employees of one contractor are temporarily stationed at another contractor's facility, the security procedures of the host contractor will govern.

(ii) USG personnel assigned to or visiting a contractor facility and engaged in oversight of an acquisition program

will retain control of their work product. Classified work products of USG employees will be handled in accordance with this rule. Contractor procedures will not require USG employees to relinquish control of their work products, whether classified or not, to a contractor.

(iii) Contractor employees at USG installations will follow the security requirements of the host. This does not relieve the contractor from security oversight of their employees who are long-term visitors at USG installations.

(b) *Classified meetings.* This paragraph applies to a conference, seminar, symposium, exhibit, convention, training course, or other such gathering during which classified information is disclosed, hereafter called a ''meeting.'' Disclosure of classified information to large diverse audiences such as conferences increases security risks. Classified disclosure at such meetings may occur when it serves a government purpose and adequate security measures have been provided in advance.

(1) *Meeting conducted by a cleared contractor.* If conducted by a cleared contractor, the meeting is authorized by a USG agency that has agreed to assume security jurisdiction. The USG agency:

(i) Must approve security arrangements, announcements, attendees, and the location of the meeting.

(ii) May delegate certain responsibilities to a cleared contractor for the security arrangements and other actions necessary for the meeting under the general supervision of the USG agency.

(2) *Request for authorization.* Contractors desiring to conduct meetings that require sponsorship will submit their requests to the USG agency that has principal interest in the subject of each meeting. Requests for authorization will include:

(i) An explanation of the USG purpose to be served by disclosing classified information at the meeting and why the use of conventional channels for release of the classified information will not advance those interests.

(ii) The subject of the meeting and scope of classified topics, to include the classification level, to be disclosed at the meeting.

(iii) The expected dates and location of the meeting.

(iv) The general content of the proposed announcement or invitation to be sent to prospective attendees or participants.

(v) The identity of any other non-government organization involved and a full description of the type of support it will provide.

(vi) A list of any foreign representatives (including their nationality, name, organizational affiliation) whose attendance at the meeting is proposed.

(vii) A description of the security arrangements necessary for the meeting to comply with the requirements of this rule.

(3) *Locations of meetings.* Classified sessions will be held only at a USG installation or a cleared contractor facility where adequate physical security and procedural controls have been approved. The authorizing USG agency is responsible for evaluating and approving the location proposed for the meeting.

(4) *Security arrangements for meetings.* The contractor will develop the security measures and procedures to be used and obtain the authorizing agency's approval. The security arrangements must provide:

(i) *Announcements.* Approval of the authorizing agency will be obtained for all announcements of the meeting.

(A) Announcements will be unclassified and will be limited to a general description of topics expected to be presented, names of speakers, and administrative instructions for requesting invitations or participation. Classified presentations will not be solicited in the announcement.

(B) When the meeting has been approved, announcements may only state that the USG agency has authorized the conduct of classified sessions and will provide necessary security assistance.

(C) The announcement will further specify that security clearances and justification to attend classified sessions are to be forwarded to the authorizing agency or its designee.

(D) Invitations to foreign persons will be sent by the authorizing USG agency.

(ii) *Clearance and need-to-know.* All persons in attendance at classified sessions will possess the requisite clearance and need-to-know for the information to be disclosed.

(A) Need-to-know will be determined by the authorizing agency or its designee based on the justification provided.

(B) Attendance will be authorized only to those persons whose security clearance and justification for attendance have been verified by the security officer of the organization represented.

(C) The names of all authorized attendees or participants must appear on an access list with entry permitted to the classified session only after verification of the attendee's identity based on presentation of official photographic identification such as a passport, contractor or USG identification card.

(iii) *Presentations.* Classified information must be authorized for disclosure in advance by the USG agency having jurisdiction over the information to be presented.

(A) Individuals making presentations at meetings will provide sufficient classification guidance to enable attendees to identify what information is classified and the level of classification.

(B) Classified presentations will be delivered orally or visually.

(C) Copies of classified presentation materials will not be distributed at the classified meeting, and any classified notes or electronic recordings of classified presentations will be classified, safeguarded, and transmitted as required by this rule.

(iv) *Physical security.* The physical security measures for the classified sessions will provide for control of, access to, and dissemination of, the classified information to be presented and will provide for secure storage capability, if necessary.

(5) *Disclosure authority at meetings.* Authority to disclose classified information at meetings, whether disclosure is by officials of industry or USG, must be granted by the USG agency or activity that has classification jurisdiction over the information to be disclosed. Each contractor that desires to disclose classified information at a meeting is responsible for requesting and obtaining disclosure approvals. Associations are not responsible for ensuring that classified presentations and papers of other organizations have been approved for disclosure. A contractor desiring to disclose classified information at a meeting will:

(i) Obtain prior written authorization for each proposed disclosure of classified information from the USG agency having jurisdiction over the information involved.

(ii) Furnish a copy of the disclosure authorization to the USG agency sponsoring the meeting.

(6) *Requests to attend classified meetings.* Before a contractor employee can attend a classified meeting, the contractor will provide justification for why the employee requires access to the classified information, cite the classified contract or GCA program or project involved, and forward the information to the authorizing USG agency.

§ 117.17 Subcontracting.

(a) *Prime contractor responsibilities.*—(1) *Responsibilities.* Before a prime contractor may release or disclose classified information to a subcontractor, or cause classified information to be generated by a subcontractor, a determination that access to classified information will be required and such access serves a legitimate USG requirement for the performance of a ''classified contract'' in accordance with § 117.9(a) must be made. Prime contractors are responsible for communicating the appropriate security requirements to all subcontractors.

(i) A ''security requirements clause'' and a ''Contract Security Classification Specification,'' or equivalent, will be incorporated in the solicitation and in the subcontract. (See the ''security requirements clause'' in the prime contract.)

(ii) The subcontractor must possess an appropriate entity eligibility determination and a classified information safeguarding capability if possession of classified information will be required.

(A) If access to classified information will not be required in the pre-award phase, prospective subcontractors are not required to possess an entity eligibility determination to receive or bid on the solicitation.

(B) If a prospective subcontractor requires access to classified information during the pre-award phase and does not have the appropriate entity eligibility determination or a classified information safeguarding capability, the prime contractor will request the CSA of the subcontractor to initiate the necessary action.

(iii) If access to classified information will not be required, the contract is not a classified contract within the meaning of this rule. If the prime contract contains requirements for release or disclosure of protected information that is not classified, such as CUI, the requirements will be incorporated in the solicitation and the subcontract and are not covered by this rule.

(2) *Prospective subcontractors entity eligibility determinations.* (i) The prime contractor will verify whether the prospective subcontractors have the appropriate entity eligibility determination and also a classified information safeguarding capability, if a subcontract requirement. This determination can be made if there is an existing contractual relationship between the parties involving classified information of the same or higher category, and must be verified by accessing the CSA-designated database, or by contacting the CSA.

(ii) If a prospective subcontractor does not have the appropriate entity eligibility determination or a classified information safeguarding capability, the prime contractor will request that the CSA of the subcontractor initiate the necessary action.

(A) Requests will include, at a minimum, the full name, address, and contact information for the requester; the full name, address, and contact information for a contact at the facility to be processed for an entity eligibility determination; the level of clearance and the required classified information safeguarding capability; and full justification for the request.

(B) Requests for safeguarding capability will include a description, quantity, end-item, and classification of the information related to the proposed subcontract.

(C) Other factors necessary to help the CSA determine if the prospective subcontractor meets the requirements of this rule will be identified, such as any special access requirements.

(3) *Lead time for entity eligibility determination when awarding to an uncleared subcontractor.* Requesting contractors will allow sufficient lead time in connection with the award of a classified subcontract to enable an uncleared bidder to be processed for the necessary entity eligibility determination. When the entity eligibility determination cannot be granted in sufficient time to qualify the prospective subcontractor for participation in the current procurement action, the CSA will continue the entity eligibility determination processing action to qualify the prospective subcontractor for future contract consideration provided:

(i) The delay in processing the entity eligibility determination was not caused by a lack of cooperation on the part of the prospective subcontractor.

(ii) Future classified negotiations may occur within 12 months.

(iii) There is reasonable likelihood the subcontractor may be awarded a classified subcontract.

(iv) *Subcontracting that involves access to FGI.* (A) A U.S. contractor may award a subcontract that involves access to FGI to another U.S. contractor after verifying with the CSA that the prospective subcontractor has the appropriate entity eligibility determination and a classified information storage capability, and review of the prime contract to determine if there are any contractual limitations for approval before awarding a subcontract. The contractor awarding a subcontract will provide appropriate security classification guidance and incorporate the pertinent security provisions in the subcontract.

(B) The contractor cannot award subcontracts involving FGI to a contractor in a third country or to a U.S. entity with a limited entity eligibility determination based on third-country FOCI without the express written consent of the originating foreign government. The CSA will coordinate with the appropriate foreign government authorities.

(b) *Security classification guidance.* (1) Prime contractors will ensure that a Contract Security Classification Specification, or equivalent, is incorporated in each classified subcontract.

(i) When preparing classification guidance for a subcontract, the prime contractor may extract pertinent information from:

(A) The Contract Security Classification Specification, or equivalent, issued with the prime contract.

(B) Security classification guides issued with the prime contract.

(C) Any security guides that provide guidance for the classified information furnished to, or that will be generated by, the subcontractor.

(ii) The Contract Security Classification Specification, or equivalent, prepared by the prime contractor will be certified by a designated official of the contractor.

(iii) In the absence of exceptional circumstances, the classification specification will not contain any classified information. If classified supplements are required as part of the Contract Security Classification Specification, or equivalent, they will be identified and forwarded to the subcontractor by separate correspondence.

(2) An original Contract Security Classification Specification, or equivalent, will be included with each RFQ, RFP, IFB, or other solicitation to ensure that the prospective subcontractor is aware of the security requirements of the subcontract and can plan accordingly. An original Contract Security Classification Specification, or equivalent, will also be included in the subcontract awarded to the successful bidder.

(3) A revised Contract Security Classification Specification, or equivalent, will be issued as necessary during the lifetime of the subcontract when the security requirements change.

(4) Requests for public release by a subcontractor will be forwarded through the prime contractor to the GCA.

(c) *Responsibilities upon completion of the subcontracts.* (1) Upon completion of the subcontract, the subcontractor may retain classified material received or generated under the subcontract for a two-year period, in accordance with the provisions in § 117.13(d)(5).

(2) If retention is required beyond the two-year period, the subcontractor must request written retention authority through the prime contractor to the GCA, including the information required by § 117.15(j).

(3) If retention authority is approved by the GCA, the prime contractor will issue a final Contract Security Classification Specification, or equivalent, annotated to provide the retention period and final disposition instructions.

(d) *Notification of invalidation, marginal, or unsatisfactory conditions.* The prime contractor will be notified if the CSA discovers marginal or unsatisfactory conditions at the subcontractor's facility or if the CSA invalidates the subcontractor's facility clearance. Once notified, the prime contractor will follow the instructions received on what action, if any, should be taken in order to safeguard classified material relating to the subcontract.

§ 117.18 Information system security.

(a) *General.* (1) Contractor information systems that are used to capture, create, store, process, or distribute classified information must be properly managed to protect against unauthorized disclosure of classified information. The contractor will implement protective measures using a risk-based approach that incorporates minimum standards for their insider threat program in accordance with CSA-provided guidance.

(2) The CSA will issue guidance based on requirements for federal systems, pursuant to 44 U.S.C. Ch. 35 of subchapter II, also known as the ''Federal Information Security Modernization Act,'' and as set forth in National Institute of Standards and Technology (NIST) Special Publication 800–37 (available at: *https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final*), Committee on National Security Systems (CNSS) Instruction 1253 (available at: *https://www.cnss.gov/CNSS/openDoc.cfm?QwPYrAJ5Ldq+s+jvttTznQ==*), and other applicable CNSS and NIST publications (*e.g.,* NIST Special Publication 800–53).

(b) *Information system security program.* The contractor will maintain an information system security program that supports overall information security by incorporating a risk-based set of management, operational, and technical security controls in accordance with CSA-provided guidance. The contractor will incorporate into the program:

(1) Policies and procedures that reduce information security risks to an acceptable level and address information security throughout the information system life cycle.

(2) Plans and procedures to assess, report, isolate, and contain data spills and compromises, to include sanitization and recovery methods.

(3) Information system security training for authorized users, as required in CSA provided guidance.

(4) Policies and procedures that address key components of the contractor's insider threat program, such as:

(i) User activity monitoring network activity, either automated or manual.

(ii) Information sharing procedures.

(iii) A continuous monitoring program.

(iv) Protecting, interpreting, storing, and limiting access to user activity monitoring automated logs to privileged users.

(5) Processes to continually evaluate threats and vulnerabilities to contractor activities, facilities, and information systems to ascertain the need for additional safeguards.

(6) Change control processes to accommodate configuration management and to identify security relevant changes that may require re-authorization of the information system.

(7) Methods to ensure users are aware of rights and responsibilities through the use of banners and user agreements.

(c) *Contractor responsibilities*—(1) *Certification.* The contractor will:

(i) Certify to the CSA that the security program for information systems to process classified information addresses management, operation, and technical controls in accordance with CSA-provided guidelines.

(ii) Provide adequate resources to the information system security program and organizationally align to ensure prompt support and successful execution of a compliant information system security program.

(2) *ISSM.* Contractors that are or will be processing classified information on an information system will appoint an employee ISSM. The contractor will confirm that the ISSM is adequately trained, has sufficient experience, and possesses technical competence commensurate with the complexity of the information system. The ISSM will:

(i) Oversee the development, implementation, and evaluation of the contractor's information system program for contractor management, information system personnel, users, and others as appropriate.

(ii) Coordinate with the contractor's insider threat senior program official so that insider threat awareness is addressed in the contractor's information system security program.

(iii) Develop, document, and monitor compliance of the contractor's information system security program in accordance with CSA-provided guidelines for management, operational, and technical controls.

(iv) Verify self-inspections are conducted at least every 12 months on the contractor's information systems that process classified information, and that corrective actions are taken for all identified findings.

(v) Certify to the CSA in writing that the systems security plan (SSP) is implemented for each authorized information systems, specified in the SSP; the specified security controls are in place and properly tested; and the information system continues to function as described in the SSP.

(vi) Brief users on their responsibilities with regard to information system security and verify that contractor personnel are trained on the security restrictions and safeguards of the information system prior to access to an authorized information system.

(vii) Develop and maintain security documentation of the security authorization request to the CSA. Documentation may include:

(A) SSPs.

(B) Security assessment reports.

(C) Plans of actions and milestones.

(D) Risk assessments.

(E) Authorization decision letters.

(F) Contingency plans.

(G) Configuration management plans.

(H) Security configuration checklists.

(I) System interconnection agreements.

(3) *Information systems security officer (ISSO).* The ISSM may assign an ISSO. If assigned, the ISSO will:

(i) Verify the implementation of the contractor's information system security program as delegated by the ISSM.

(ii) Ensure continuous monitoring strategies and verify corrective actions to the ISSM.

(iii) Conduct self-inspections and verify corrective actions to the ISSM.

(4) *Information system users.* All information system users will:

(i) Comply with the information system security program requirements as part of their responsibilities for protecting classified information.

(ii) Be accountable for their actions on an authorized information system.

(iii) Not share any authentication mechanisms (including passwords) issued for the control of their access to an information system.

(iv) Protect authentication mechanisms at the highest classification level and most restrictive classification category of information to which the mechanisms permit access.

(v) Be subject to monitoring of their activity on any classified network, understanding that the results of such monitoring can be used against them in a criminal, security, or administrative proceeding or action.

(vi) Notify the ISSM or ISSO when access to a classified system is no longer required.

(d) *Information system security life-cycle.* The CSA-provided guidance on the information system security life-cycle is based on the risk management framework outlined in NIST special publication 800–37 that emphasizes:

(1) Building security into information systems during initial development.

(2) Maintaining continuous awareness of the current state of information system security.

(3) Keeping contractor management informed to facilitate risk management decisions.

(4) Supporting reciprocity of information system authorizations.

(e) *Risk management framework.* The risk management framework is a seven-step process used for managing information system security-related risks. These steps will be used to help ensure security capabilities provided by the selected security controls are implemented, tested, validated, and approved by the USG authorizing official with a degree of assurance appropriate for the information system. This process accommodates an on-going risk mitigation strategy.

(1) *Prepare.* The contractor will execute essential activities at the organization, mission and business process, and system levels of the organization to help prepare the organization to manage its security and privacy risks using the Risk Management Framework.

(2) *Categorize.* The contractor will categorize the information system and the information processed, stored, and transmitted by the information system based on an impact analysis. Unless imposed by contract, the information system baseline is moderate-confidentiality, low-integrity, and low-availability.

(3) *Select.* The contractor will select an initial set of baseline security controls for the information system based on the security categorization; tailoring and supplementing the security control baseline as needed based on an organizational assessment of risk and local conditions.

(4) *Implement.* The contractor will implement the security controls and document how the controls are deployed within the information system and the operational environment.

(5) *Assess.* The contractor will assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system. The contractor will review and certify to the CSA that all systems have the appropriate protection measures in place.

(6) *Authorize.* The CSA will use the information provided by the contractor to make a timely, credible, and risk-based decision to authorize the system to process classified information. The CSA must authorize the system before the contractor can use the system to process classified information.

(7) *Monitor.* The contractor will monitor and assess selected security controls in the information system on an ongoing basis:

(i) Effectiveness of security controls.

(ii) Documentation of changes to the information system and the operational environment.

(iii) Analysis of the security impact of changes to the information system.

(iv) Making appropriate reports to the CSA.

(f) *Unclassified information systems that process, store, or transmit CUI.* While outside the requirements of the NISPOM, contractors will comply with contract requirements regarding contractor information systems that process, store, or transmit CUI.

§ 117.19 International security requirements.

(a) *General.* This section provides information and procedures governing the protection of classified information in international programs.

(b) *Disclosure of classified U.S. information to foreign interests.*—(1) *Applicable federal law.* The transfer of articles, services, and related data to a foreign person, within or outside the United States, or the movement of such material or information to any destination outside of the legal jurisdiction of the United States constitutes an export. Depending on the nature of the articles or data, most exports are pursuant to (1) 22 U.S.C. chapter 39, also known and referred to in this rule as the ''Arms Export Control Act,'' (2) 50 U.S.C. 4801 *et seq.,* also known as the ''Export Control Reform Act of 2018,'' or (3) the AEA. This section applies to those exports that involve classified information.

(2) *Security agreements.*—(i) Bilateral security agreements (*e.g.,* General Security of Information Agreements and General Security of Military Information Agreements) are negotiated with various foreign governments. Confidentiality requested by some foreign governments prevents a listing of the countries that have executed these agreements. The bilateral security agreement, negotiated through diplomatic channels:

(A) Requires that each government provide substantially the same degree of protection to classified information released by the other government.

(B) Contains provisions concerning limits on the use of each government's information, including restrictions on third-party transfers and proprietary rights.

(C) Does not commit governments to share classified information, nor does it constitute authority to release classified material to that government.

(D) Satisfies, in part, the eligibility requirements of the Arms Export Control Act concerning the agreement of the recipient foreign government to protect U.S. classified defense articles and classified information.

(ii) The applicable CSA will provide a mechanism for contractors to access, for official purposes, classified general security agreements.

(iii) Industrial security agreements have been negotiated with certain foreign governments that identify the procedures to be used when foreign government classified information is provided to U.S. industry and UUSG classified information is provided to foreign defense industry.

(3) *Authorization for disclosure.* The GCA will provide disclosure guidance.

(i) Contractors will only disclose non-public USG information to foreign persons in accordance with specified requirements of the contract. In the absence of any specified requirements the contractor will not disclose non-public USG information to foreign persons.

(ii) Disclosure authorization may be in the form of an export license or other export authorization by a cognizant export authority.

(iii) The contractor may not use disclosure guidance provided by the GCA for a previous contract or program unless so instructed in writing by the GCA or the licensing authority.

(iv) Disclosure and export of classified information, authorized by an appropriate USG disclosure official, by a contractor will ensure the following:

(A) *International agreements.* Contractors may not disclose classified information until agreements are signed by the participating government and disclosure guidance and security arrangements are established. The export of technical data pursuant to such agreements may be exempt by approval of the Department of State or the Department of Commerce.

(B) *Symposia, seminars, exhibitions, and conferences.* Contractors must assure that any foreign nationals who will be attending a classified gathering have the appropriate export license, disclosure authority, and security assurance on file.

(C) *Visits by foreign nationals to the contractor.* The contractor will limit disclosure of classified information to that specific information authorized in connection with an approved visit request and an export authorization, as required.

(D) *Temporary exports.* Classified articles, including articles that require the use of classified information for operation, exported for demonstration purposes must remain under U.S. control. The contractor must obtain an export authorization from the relevant authority (*i.e.,* from the Department of State in accordance with 22 CFR parts 120–130, also known as and referred to in this rule as the ''International Traffic in Arms Regulations,'' or from the Department of Commerce in accordance with 15 CFR parts 730–774, also known as the ''Export Administration Regulations'').

(4) *Direct commercial arrangements.* (i) The disclosure of classified information may be authorized pursuant to a direct commercial sale with the appropriate export authorization. A direct commercial arrangement includes sales, loans, leases, or grants of classified items, including sales under a government agency sales financing program.

(ii) If a proposed disclosure is in support of a foreign government requirement, the contractor should consult with U.S. in-country officials, normally the U.S. Security Assistance/Armaments Cooperation Office or Commercial Counselor.

(A) Before a contractor makes a proposal to a foreign interest that involves the eventual disclosure of U.S. classified information, the contractor must obtain appropriate government disclosure authorization.

(B) Such disclosure authorization does not equate with authorization for export. Export authorization must be obtained from the appropriate regulatory body.

(iii) The contractor will request a FCL assurance for a foreign entity through the CSA from the security authority of the foreign entity's sponsoring government prior to entering into a contractual arrangement with the foreign entity.

(5) *Subcontract security provisions.* (i) A U.S. contractor may be authorized to enter into an agreement involving classified information with a foreign contractor. The U.S. contractor's empowered official will verify the contractor can release the information to a foreign person. Such agreements may include:

(A) Award of a subcontract.

(B) Department of State authorized manufacturing license agreement, technical assistance agreement, or other direct commercial arrangement.

(ii) The contractor will incorporate security provisions into the subcontract document or agreement, and provide security classification guidance by means of a Contract Security Classification Specification, or equivalent.

(iii) The contractor will provide a copy of the signed contract with the provisions and the classification guidance to the CSA.

(iv) If the export authorization specifies that additional security arrangements are necessary for performance on the contract, the contractor will incorporate those additional arrangements by appropriate provision in the contract or in a separate security document.

(v) The contractor will prepare and maintain a written record that identifies the originator or source of classified information that will be used in providing classified defense articles, material or services to foreign customers. The contractor will maintain this listing with the contractor's record copy of the pertinent export authorization.

(vi) The contractor will include the security provisions in accordance with paragraph (b)(5) in this section in all contracts and subcontracts involving classified information that are awarded to foreign contractors. Contractors must insert the bracketed contract specific information (*e.g.,* applicable country and disposition of classified material) where noted, when using the following security clauses in the contract.

(A) All classified information and material furnished or generated under the contract will be protected to ensure that:

(*1*) The recipient will not release the information or material to any third party without disclosure authorization and export authorization, as appropriate.

(*2*) The recipient will afford the information and material a degree of protection equivalent to that afforded it by the releasing government.

(*3*) The recipient will not use the information and material for other than the purpose for which it was furnished without the prior written consent of the releasing government.

(B) Classified information and material furnished or generated under this contract will be transferred through government channels or other channels specified in writing by the governments of the United States and [insert applicable country]. It will only be transferred to persons who have an appropriate security clearance and an official need for access to the information in order to perform on the contract.

(C) Classified information and material furnished under the contract will be re-marked by the recipient with its government's equivalent security classification markings.

(D) Classified information and material generated under the contract must be assigned a security classification as specified by the Contract Security Classification Specifications, or equivalent, provided with this contract.

(E) All cases in which it is known or there is reason to believe that classified information or material furnished or generated under the contract has been lost or disclosed to unauthorized persons will be reported promptly and fully by the contractor to its government's security authorities.

(F) Classified information and material furnished or generated pursuant to the contract will not be further provided to another potential contractor or subcontractor unless:

(*1*) A potential contractor which is located in the United States or [insert applicable country] has been approved for access to classified information and material by the USG or [insert applicable country] security authorities; or

(*2*) If located in a third country, prior written USG consent is obtained.

(G) Upon completion of the contract, all classified material furnished or generated pursuant to the contract will be [insert whether the material is to be returned or destroyed, or provide other instructions].

(H) The recipient contractor will insert terms that substantially conform to the language of these provisions, including this one, in all subcontracts under this contract that involve access

to classified information furnished or generated under this contract.

(c) *FGI.*—(1) *General.* The contractor will notify the csa when awarded contracts by a foreign interest that will involve access to classified information. The csa will oversee and ensure implementation of the security requirements of the contract on behalf of the foreign government, including the establishment of channels for the transfer of classified material.

(2) *Contract security requirements.* The foreign entity that awards a classified contract is responsible for providing appropriate security classification guidance and any security requirements clauses. The contractor will report to the CSA when a foreign entity fails to provide classification guidance.

(3) *Marking foreign government classified material.* Foreign government classified material will be marked in accordance with § 117.14(l).

(4) *Foreign Government RESTRICTED Information and ''In Confidence'' Information.* Foreign government RESTRICTED information and ''in confidence'' information will be marked in accordance with § 117.14(m).

(5) *Marking U.S. documents containing FGI.* U.S. documents containing FGI will be marked in accordance with § 117.14(n).

(6) *Marking documents prepared for foreign governments.* Marking documents prepared for foreign governments will be marked in accordance with § 117.14(o).

(7) *Storage and control.* Contractors will store foreign government material and control access generally in the same manner as U.S. classified material of an equivalent classification. Contractors will store foreign government material in a manner that will separate it from other material. Separation can be accomplished by establishing distinct files in a storage container or on an information system.

(8) *Disclosure and use limitations.* (i) FGI is provided by the foreign government to the United States. The contractor will:

(A) Not disclose FGI to nationals of a third country, or to any other third party, or use it for any purpose other than that for which it was provided without the prior written consent of the originating foreign government.

(B) Submit requests for other uses or further disclosure to the GCA for U.S. contracts, and through the CSA for direct commercial contracts.

(ii) Approval of the request by the foreign government does not eliminate the requirement for the contractor to obtain an export authorization.

(9) *Transfer.* The contractor will transfer FGI within the United States and its territories using the same channels as specified for U.S. classified information of an equivalent classification, except that contractors cannot use non-cleared express overnight carriers for FGI.

(10) *Reproduction.* The reproduction of foreign government TOP SECRET or equivalent information requires the written approval of the originating government.

(11) *Disposition.* The contractor:

(i) Will destroy FGI on completion of the contract unless the contract specifically authorizes retention or return of the information to the U.S. GCA or foreign government that provided the information.

(ii) Must witness the destruction of TOP SECRET, execute a destruction certificate, and retain the destruction certificate for two years.

(12) *Reporting of improper receipt of foreign government material.* The contractor will report improper receipt of foreign government material in accordance with § 117.8(c)(13).

(13) *Subcontracting.* Subcontracting procedures will be in accordance with § 117.17(a)(4).

(d) *International transfers of classified material.*—(1) *General.* This paragraph (d) contains the procedures for international transfers of classified material through government-to-government channels or other arrangements agreed to by the governments involved, otherwise referred to as government-to-government transfers. The requirements in this paragraph (d) do not apply to the transmission of classified material to usg activities outside the united states.

(i) All international transfers of classified material must take place through channels approved by both governments. U.S. control of classified material must be maintained until the material is officially transferred to the intended recipient government through its designated government representative (DGR).

(ii) To ensure government control, written transmission instructions must be prepared for all international transfers of classified material. The contractor is responsible for the preparation of instructions for direct commercial arrangements, and the GCA will prepare instructions for government arrangements.

(iii) The contractor will contact the CSA at the earliest possible stage in deliberations that will lead to the international transfer of classified material. The CSA will advise the contractor on the transfer arrangements, identify the recipient government's DGR, appoint a U.S. DGR, and ensure that the transportation plan prepared by the contractor or foreign government is adequate.

(iv) The contractor's empowered official is responsible for requests for all export authorizations, including ones that will involve the transfer of classified information.

(2) *Transfers of freight.*—(i) *Transportation plan (TP).* (A) A requirement to prepare a TP will be included in each arrangement that involves the international transfer of classified material as freight. The TP will:

(*1*) Describe requirements for the secure shipment of the material from the point of origin to the ultimate destination.

(*2*) Provide for security requirements in the event the transfer cannot be made promptly.

(B) The U.S. and recipient government DGRs will be identified in the TP as well as any requirement for an escort. When there are to be repetitive shipments, a notice of classified consignment will be used.

(ii) *Government agency arrangements.* Classified material to be furnished to a foreign government under such transactions normally will be shipped via government agency-arranged transportation and be transferred to the foreign government's DGR within the recipient government's territory.

(A) The government agency that executes the arrangement is responsible, in coordination with the recipient foreign government, for preparing a TP.

(B) When the point of origin is a U.S. contractor facility, the GCA will provide the contractor with a copy of the TP and the applicable letter of offer and acceptance. If a freight forwarder will be involved in processing the shipment, the GCA will provide a copy of the TP to the freight forwarder.

(C) *Commercial arrangements.* (*1*) The contractor will prepare a TP in coordination with the receiving government. This requirement applies whether the material is moved by land, sea, or air, and applies to U.S. and foreign classified contracts.

(*2*) After the CSA approves the TP, the CSA will forward it to the recipient foreign government security authorities for final coordination and approval. The CSA will notify the contractor upon the concurrence by the respective parties.

(D) *International carriers.* The international transfer of classified material will be made using only ships, aircraft, or other carriers that:

(*1*) Are owned or chartered by the USG or under U.S. registry;

(*2*) Are owned or chartered by or under the registry of the recipient government; or

(*3*) Are other than those described that are expressly authorized to perform this function in writing by the Designated Security Authority of the GCA and the security authorities of the foreign government involved. This authority cannot be delegated and this exception may be authorized only when a carrier described in paragraph (d)(2)(iv)(A) or (d)(2)(iv)(B) in this section is not available and an urgent operational requirement dictates use of the exception.

(E) *Escorts.* (*1*) The contractor must provide escorts for international shipments of SECRET or CONFIDENTIAL material by air.

(*2*) Escorts must have an eligibility determination and access to classified information at the classification level of the material being shipped.

(*3*) Escorts are responsible for ensuring that the classified material being shipped is safeguarded in the event of an emergency stop en route, re-routing of the aircraft, or in the event that the recipient government's representative fails to meet the shipment at its destination.

(*4*) The contractor does not have to provide escorts if:

(*i*) The classified material is shipped by the Defense Transportation System or a U.S. military carrier.

(*ii*) The recipient government DGR has signed for the receipt of the classified material within the United States.

(*iii*) The classified material is shipped via a military carrier of the recipient government or a carrier owned by or registered to the recipient government.

(*iv*) The classified material is shipped via a cleared U.S. commercial freight carrier, so long as the contractor has a written agreement from the U.S. commercial freight carrier to provide an escort who is eligible for access to classified information and has access to classified information at the classification level of the material being shipped.

(*v*) There are exceptional circumstances, and procedures have been approved by both the USG and the recipient government.

(3) *Secure communications plan.* (i) The contractor is required to meet all requirements outlined in this section, as applicable, for the secure communications plan.

(ii) The secure communications plan may be approved within a program security instruction, SSP, or a government to government agreement by the designated security authorities. A separate memorandum of understanding or memorandum of agreement is not required.

(iii) Additionally, an SSP must be authorized in accordance with § 117.18 and the CSA provided guidance.

(4) *Return of material for repair, modification, or maintenance.* (i) A foreign government or foreign contractor may return classified material to a U.S. contractor for repair, modification, or maintenance.

(ii) The approved methods of return will be specified in either the GCA sales arrangement, the security requirements section of a direct commercial sales arrangement or, in the case of material transferred as freight, in the original TP.

(iii) The contractor, on receipt of notification that classified material is to be received, will notify the applicable CSA.

(5) *Use of freight forwarders.* (i) A commercial freight forwarder may be used to arrange for the international transfer of classified material as freight.

(A) The freight forwarder must be under contract to a USG agency, U.S. contractor, or the recipient foreign government.

(B) The contract will describe the specific functions to be performed by the freight forwarder.

(C) The responsibility for security and control of the classified material that is processed by freight forwarders remains with the USG until the freight is transferred to a DGR of the recipient government.

(ii) Only freight forwarders that have a valid determination of eligibility for access to classified information and storage capability for classified material at the appropriate level are eligible to take custody or possession of classified material for delivery as freight to foreign recipients. Freight forwarders that only process unclassified paperwork and make arrangements for the delivery of classified material to foreign recipients do not require an eligibility determination for access to classified information.

(iii) A freight forwarder cannot serve as a DGR.

(6) *Hand carrying classified material.* To meet contractual requirements, the CSA may authorize contractor employees to hand carry classified material outside the United States. SECRET is the highest level of classified material to be carried and it must be of such size and weight that the courier can retain it in his or her possession at all times.

(i) The CSA will ensure that the contractor has made necessary arrangements with U.S. airport security and customs officials and that security authorities of the receiving government approve the plan. If the transfer is under a contract or a bilateral or multinational government program, the GCA will approve the request in writing. The contractor will notify the CSA of a requirement to hand carry at least 5 working days in advance of the transfer.

(ii) The courier must be a full-time employee of the dispatching or receiving contractor who has been determined eligible and has been granted access to classified information.

(iii) The employing contractor will provide the courier with a courier certificate that is consecutively numbered and valid for one journey only. The journey may include more than one stop if approved by the CSA and secure government storage has been arranged at each stop. The courier will return the courier certificate to the dispatching contractor immediately on completion of the journey.

(iv) Before commencement of each journey, the courier will read and initial the notes to the courier attached to the courier certificate and sign the courier declaration. The contractor will maintain the declaration until completion of the next CSA security review.

(v) The dispatching contractor will inventory, wrap, and seal the material in the presence of the U.S. DGR. The contractor will place the address of the receiving security office and the return address of the dispatching contractor security office on the inner envelope or wrapping and mark it with the appropriate classification. The contractor will place the address of the receiving government's DGR on the outer envelope or wrapping along with the return address of the dispatching contractor.

(vi) The dispatching contractor will prepare three copies of a receipt based on the inventory and list the classified material that is being sent. The dispatching contractor will retain one copy of the receipt. The contractor will pack the other two copies with the classified material. The contractor will obtain a receipt for the sealed package from the courier.

(vii) The dispatching contractor will provide the receiving contractor with 24 work hours advance notification of the anticipated date and time of the courier's arrival and the identity of the courier. The receiving contractor must notify the dispatching contractor if the courier does not arrive within 8 hours of the expected time of arrival. The dispatching contractor will notify its DGR of any delay, unless officially notified otherwise of a change in the courier's itinerary.

(viii) The receiving DGR will verify the contents and sign the receipts enclosed in the consignment. The receiving DGR will return one copy to the courier. On return, the courier will provide the executed receipt to the dispatching contractor.

(ix) Throughout the journey, the courier will maintain the classified material under direct personal control. The courier will not leave the material unattended at any time during the journey, in the transport being used, in hotel rooms, in cloakrooms, or other such location, and will not deposit it in hotel safes, luggage lockers, or in luggage offices. In addition, the courier will not open envelopes or packages containing the classified material en route, unless required by customs or other government officials.

(x) When inspection by government officials is unavoidable, the courier will request that the officials provide written verification that they have opened the package. The courier will notify their employing contractor as soon as possible. The contractor will notify the U.S. DGR. If the inspecting officials are not of the same country as the dispatching contractor, the CSA will notify the designated security authority in the country whose officials inspected the consignment. Under no circumstances will the courier hand over the classified material to customs or other officials for their custody.

(xi) When carrying classified material, the courier will not travel by surface routes through third countries, except as authorized by the CSA. The courier will travel only on carriers described in paragraph (d)(2)(iv) in this section, and will travel direct routes between the United States and the destination.

(7) *Classified material receipts.* (i) The U.S. DGR and the DGR of the ultimate foreign recipient will maintain a continuous chain of receipts to record international transfers of all classified material from the contractor through the dispatching DGR and recipient DGR to the ultimate foreign recipient. The dispatching contractor will retain:

(A) An active suspense record until return of applicable receipts for the material.

(B) A copy of the external receipt that records the passing of custody of the package containing the classified material and each intermediate consignee in a suspense file until the receipt that is enclosed in the package is signed and returned.

(ii) The contractor will initiate follow-up action through the CSA if the signed receipt is not returned within 45 days.

(8) *Contractor preparations for international transfers of classified material pursuant to direct commercial and foreign military sales.* To prepare for international transfers the contractor will:

(i) Identify each party to be involved in the transfer in the applicable contract or agreement and in the license application or letter request.

(ii) Notify the appropriate U.S. DGR when the material is ready.

(iii) When the classified material is also ITAR-controlled, provide documentation or written certification by an empowered official (as defined in the ITAR) to the U.S. DGR. This documentation must verify that the classified shipment is within the limitation scope of the pertinent export authorization or an authorized exemption to the export authorization requirements, or is within the limitations of the pertinent GCA contract.

(iv) Have the classified shipment ready for visual review and verification by the DGR. As a minimum this will include:

(A) Preparing the packaging materials, address labels, and receipts for review.

(B) Marking the contents with the appropriate U.S. classification or the equivalent foreign government classification, downgrading, and declassification markings, as applicable.

(C) Ensuring that shipping documents (including, as appropriate, the shipper's export declaration) include the name and contact information for the CSA that validates the license or letter authorization, and the FSO or designee for the particular transfer.

(D) Sending advance notification of the shipment to the CSA, the recipient, and to the freight forwarder, if applicable. The notification will require that the recipient confirm receipt of the shipment or provide notice to the contractor if the shipment is not received in accordance with the prescribed shipping schedule.

(9) *Transfers pursuant to an ITAR exemption.* (i) The contractor will provide to the DGR valid documentation (*i.e.,* license, export authorization, letter of offer and acceptance, or agreement) to verify the export authorization for classified technical data information or certain defense articles to be transferred under an exemption to the ITAR exemption. The documentation must include a copy of the Department of State Form DSP–83 associated with the original export authorization.

(ii) Classified technical data information or certain defense articles to be exported pursuant to ITAR exemptions will be supported by a written authorization signed by an authorized exemption official or exemption certifying official who has been appointed by the GCA's responsible disclosure authority.

(A) The contractor will provide a copy of the authorization to the CSA.

(B) The CSA will provide a copy of the authorization to the Department of State Directorate of Defense Trade Controls (DDTC).

(e) *International visits.*—(1) *General.* (i) The contractor will establish procedures to monitor international visits by their employees and visits or assignments of foreign nationals to the contractor location. Doing so will ensure that the disclosure of, and access to, classified export-controlled articles related to classified information are limited to those that are approved by an export authorization.

(ii) Contractors cannot use visit authorizations to employ or otherwise acquire the services of foreign nationals that require access to export-controlled information. An export authorization is required for such situations.

(2) *International visits by U.S. contractor employees.*—(i) *Types and purpose of international visits.*—(A) *One-time visits.* A visit for a single, short-term occasion (normally 30 days or fewer) for a specified purpose.

(B) *Recurring visits.* Intermittent, recurring visits over a specified period of time, normally up to one year in duration, in support of a government-approved arrangement, such as an agreement, contract, or license. By agreement of the governments, the term of the authorization may be for the duration of the arrangement, subject to annual review, and validation.

(C) *Long-term visits.* A single visit for an extended period of time, normally up to one year, in support of an agreement, contract, or license.

(D) *Emergency visits.* A visit related to a specific government-approved contract, international agreement or announced request for proposal, and failure to make the visit could be reasonably expected to seriously jeopardize performance on the contract or program, or result in the loss of a contract opportunity.

(ii) *Requests for visits.* Visit requests are necessary to make administrative arrangements and disclosure decisions and obtain security assurances.

(A) Many foreign governments require the submission of a visit request for all visits to a government facility or a cleared contractor facility, even though classified information may not be involved. They may also require that the requests be received a specified number of days in advance of the visit.

(B) The contractor can obtain information pertaining to the visit

requirements of other governments and the NATO from the CSA. The contractor must obtain an export authorization if classified export controlled articles or technical data is to be disclosed or if information to be divulged is related to a classified USG program, unless the disclosure of the information is covered by other agreements, authorizations, or exemptions.

(iii) *Request format.* Contractors will request a visit request template from the CSA. The contractor will forward the visit request to the security official designated by the CSA. The host for the visit should coordinate the visit in advance with appropriate government authorities who are required to approve the visit. It is the visitor's responsibility to ensure that such coordination has occurred.

(iv) *Government agency programs.* The contractor will submit a visit request when contractor employees are to visit foreign government facilities or foreign contractors on USG orders in support of a government contract or agreement.

(v) *Requests for emergency visits.* The requester will include in the emergency visit request, and any other requirements in accordance with applicable CSA guidance:

(A) The complete name, position, address, and telephone number of the person to be visited.

(B) A knowledgeable foreign government point of contact.

(C) The identification of the contract, agreement, or program and the justification for submission of the emergency visit request.

(vi) *Requests for recurring visits.* Contractors will request recurring visit authorizations at the beginning of each program. After approval of the request, the contractor may arrange individual visits directly with the security office of the location to be visited subject to 5 working days advance notice.

(vii) *Amendments.* (A) Once visit requests have been approved or are being processed, the contractor may amend them only to change, add, or delete names and change dates.

(B) The contractor cannot amend visit requests to specify dates that are earlier than originally specified.

(C) The contractor cannot amend emergency visit authorizations.

(3) *Classified visits by foreign nationals to U.S. contractors.*—(i) *Requests for classified visits.* Requests for visits by foreign nationals to U.S. contractors that will involve the disclosure of classified information may require authorization by the Department of State. Classified visits by foreign nationals must be processed by government national security authorities on behalf of the contractor through the sponsoring foreign government (normally the visitor's embassy) to the USG for approval.

(ii) *USG approval.* The USG may approve or deny the request or decline to render a decision.

(A) *USG-Approved Visits.* (*1*) USG approved classified visits cannot be used to avoid the export licensing requirements for commercial initiatives.

(*2*) When the cognizant USG agency approves a classified visit, the notification of approval will contain instructions on the level and scope of classified and unclassified information authorized for disclosure, as well as any limitations.

(*3*) Final acceptance for the visit will be subject to the concurrence of the contractor. The contractor will notify the USG agency when a classified visit is not desired.

(B) *Visit request denials.* (*1*) If the USG agency does not approve the disclosure of the information related to the proposed classified visit, it will deny the classified visit request. The USG agency will advise the requesting government and the contractor to be visited of the reason for the denial.

(*2*) The contractor may accept the visitor(s), but only information that is in the public domain may be disclosed during the classified visit.

(C) *Non-sponsorship.* The USG agency will decline to render a decision on a classified visit request that is not in support of a USG program. The USG agency will furnish a declination notice indicating that the classified visit is not USG-approved (*i.e.,* the classified visit is non-sponsored) to the requesting foreign government with an information copy to the U.S. contractor to be visited.

(*1*) A declination notice does not preclude the classified visit, provided the contractor has, or obtains, an export authorization for the information involved and, has been notified that the requesting foreign government has provided the required security assurance of the proposed visitor to the USG agency in the original classified visit request.

(*2*) It is the contractor's responsibility to consult applicable export regulations to determine licensing requirements regarding the disclosure of export-controlled information during such classified visits by foreign nationals.

(D) *Visits to subsidiaries.* A classified visit request authorization for a classified visit to any element of a corporate family may be used for visits to other divisions or subsidiaries within the same corporate family in accordance with § 117.15(h)(3), provided disclosures are for the same purpose and the information to be disclosed does not exceed the parameters of the approved classified visit request.

(E) *Long-term classified visits and assignments of foreign nationals.* Extended classified visits and assignments of foreign nationals to contractor locations can be authorized only when it is essential pursuant to a contract or government agreement (*e.g.,* joint venture, liaison representative to a joint or multinational program, and direct commercial sale). The contractor will:

(*1*) Consult with its empowered official for guidance.

(*2*) Notify the CSA in advance of all long-term classified visits and assignments of foreign nationals.

(*3*) Provide the CSA with a copy of the approved classified visit authorization or the USG export authorization.

(4) *Control of foreign visitors to U.S. contractors.*—(i) *Contractor.* The contractor will:

(A) Establish procedures to ensure that foreign visitors are not afforded access to classified information except as authorized by an export license, approved visit request, or other exemption to the licensing requirements.

(B) Not inform the foreign visitor of the scope of access authorized or of the limitations imposed by the government.

(ii) *Foreign visitors.* Foreign visitors will not be given custody of classified material except when they are acting as official couriers of the government and the CSA authorizes the transfer.

(iii) *Visitor records.* The contractor will maintain a record of foreign visitors for one year when the visit involves access to classified information.

(iv) *Temporary approval of safeguarding.* (A) Classified U.S. and foreign government material at a U.S. contractor location is to remain under U.S. contractor custody and control and is subject to self-inspection and CSA security reviews.

(B) This does not preclude the contractor from furnishing a foreign visitor with a security container for the temporary storage of classified material, consistent with the purpose of the visit or assignment, provided the CSA approves and responsibility for the container and its contents remains with the U.S. contractor.

(*1*) The CSA may approve exceptions to this policy on a case-by-case basis for the storage of foreign government classified information furnished to the visitor by the visitor's government through government channels.

(*2*) The CSA must approve such exceptions in advance in writing with

agreement from the visitor's government. The agreed procedures will be included in the contractor's TCP, will require the foreign nationals to provide receipts for the material, and will include an arrangement for the CSA to ensure compliance, including provisions for the CSA to inspect and inventory the material.

(v) *TCP.* A TCP is required to control access by foreign nationals assigned to, or employed by, cleared contractor facilities, and when foreign nationals visit cleared contractor facilities on a long-term or extended basis, unless the CSA determines that procedures already in place at the contractor's facility are adequate. The TCP will contain procedures to control access for all export-controlled information. A sample TCP may be obtained from the CSA.

(f) *Contractor operations abroad.*—(1) *Access by contractor employees assigned outside the United States.* (i) Contractor employees assigned outside the United States, its possessions, or territories may have access to classified information in connection with performance on a specified U.S., NATO, or foreign government classified contract.

(ii) The assignment of an employee who is a non-U.S. citizen outside the United States on programs that will involve access to classified information is prohibited.

(2) *Storage, custody, and control of classified information abroad by contractor employees.* (i) The USG is responsible for the storage, custody, and control of classified information required by a U.S. contractor employee abroad. Therefore, the storage of classified information by contractor employees at any location abroad that is not under USG control is prohibited. The storage may be at a U.S. military facility, an American Embassy or consulate, or other location occupied by a USG organization.

(ii) A contractor employee may be furnished a security container to temporarily store classified material at a USG agency overseas location. The decision to permit a contractor to temporarily store classified information must be approved in writing by the senior security official for the USG host organization.

(iii) A contractor employee may be permitted to temporarily remove classified information from an overseas USG-controlled facility when necessary for the performance of a GCA contract or pursuant to an approved export authorization.

(A) The responsible USG security official at the facility will verify that the contractor has an export authorization or other written USG approval to have the material, verify the need for the material to be removed from the facility, and brief the employee on handling procedures.

(*1*) In such cases, the contractor employee will sign a receipt for the classified material.

(*2*) Arrangements will also be made with the USG custodian for the return and storage of the classified material during non-duty hours.

(B) The security office at the USG facility will report violations of this policy to the applicable CSA.

(iv) A contractor employee will not store classified information at overseas divisions or subsidiaries of U.S. entities incorporated or located in a foreign country.

(A) The divisions or subsidiaries may possess classified information that has been transferred to the applicable foreign government through government-to-government channels pursuant to an approved export authorization or other written USG authorization.

(B) Access to this classified information at such locations by a U.S. contractor employee assigned abroad by the parent facility on a visit authorization in support of a foreign government contract or subcontract, is governed by the laws and regulations of the country in which the division or subsidiary is registered or incorporated. The division or subsidiary that has obtained the information from the foreign government will provide the access.

(v) U.S. contractor employees assigned to foreign government or foreign contractor locations under a direct commercial sales arrangement will be subject to the host-nation's industrial security policies.

(3) *Transmission of classified material to employees abroad.* The transmission of classified material to a cleared contractor employee located outside the United States will be through USG channels.

(i) If the material is to be used for other than USG purposes, an export authorization is required and a copy of the authorization, validated by the DGR, will accompany the material. The material will be addressed to a U.S. military organization or other USG organization (*e.g.,* an embassy).

(ii) USG organization abroad will be responsible for custody and control of the material.

(4) *Security briefings.* An employee being assigned outside the United States will be briefed on the security requirements of his or her assignment, including the handling, disclosure, and storage of classified information overseas.

(g) *NATO information security requirements.*—(1) *General.* This section provides the security requirements needed to comply with the procedures established by the U.S. Security Authority for NATO Affairs Instruction 1–07 (available at: *http://archives.nato.int/informationobject/browse?topLod=0&query=United+States+Security+Authority+for+NATO+Affairs+Instruction+1-07*) for safeguarding NATO information provided to U.S. industry.

(2) *NATO security classification levels.*

TABLE 1 TO PARAGRAPH (g)(2) NATO SECURITY CLASSIFICATION LEVELS

NATO security classification	Classification level
COSMIC TOP SECRET	Top Secret.
NATO SECRET	Secret.
NATO CONFIDENTIAL	Confidential.
NATO RESTRICTED [1]	Does not correspond to an equivalent U.S. classification.

[1] Pursuant to applicable NATO security regulations and United States Security Authority, NATO Instruction 1–07, security accreditation may be delegated to contractors for information systems processing only NATO RESTRICTED information. The contractor will be responsible for executing specific provisions under contract for the accreditation of such systems, and shall provide the Contracting Authority with a written statement confirming the information system has been accredited in compliance with the minimum requirements established in the contract security clause or contract Security Aspects Letter.

(3) *ATOMAL Classification Markings.* ATOMAL is a marking applied to U.S. RESTRICTED DATA or FORMERLY RESTRICTED DATA and UK Atomic information that has been released to the NATO.

TABLE 2 TO PARAGRAPH (g)(3) ATOMAL CLASSIFICATION MARKINGS

ATOMAL marking	Classification level
COSMIC TOP SECRET ATOMAL	Top Secret.
NATO SECRET ATOMAL	Secret.
NATO CONFIDENTIAL ATOMAL	Confidential.

(4) *NATO contracts.* NATO contracts involving NATO-unique systems, programs, or operations are awarded by a NATO Production and Logistics Organization (NPLO), a designated NATO Management Agency, the NATO Research Staff, or a NATO Command. In the case of NATO infrastructure projects (*e.g.,* airfields, communications), the NATO contract is awarded by a contracting agency or prime contractor of the NATO nation responsible for the infrastructure project.

(5) *NATO facility security clearance certificate (FSCC).* A NATO FSCC is required for a contractor to negotiate or perform on a NATO classified contract.

(i) A U.S. entity qualifies for a NATO FSCC if it has an equivalent U.S. entity eligibility determination and its personnel have been briefed on NATO procedures.

(ii) The CSA will provide the NATO FSCC to the requesting activity.

(iii) A NATO FSCC is not required for GCA contracts involving access to NATO classified information.

(6) *Eligibility for personnel access to classified information.* Access to NATO classified information requires a final determination that an individual is eligible for access to classified information at the equivalent level.

(7) *NATO briefings.* Before having access to NATO classified information, the contractor will give employees a NATO security briefing that covers the requirements of this section and the consequences of negligent handling of NATO classified information. A representative of the CSA will give the initial briefing to the contractor. The contractor must conduct annual refresher briefings.

(i) When access to NATO classified information is no longer required, the contractor will debrief the employees. The employees will sign a certificate stating that they have been briefed or debriefed, as applicable, and acknowledge their responsibility for safeguarding NATO information.

(ii) The contractor will maintain certificates for two years for NATO SECRET and CONFIDENTIAL, and three years for COSMIC TOP SECRET and all ATOMAL information. The contractor will maintain a record of all NATO briefings and debriefings in the CSA-designated database.

(8) *Access to NATO classified information by foreign nationals.* Foreign nationals of non-NATO nations may have access to NATO classified information only with the consent of the NATO Office of Security and the contracting activity.

(i) Requests will be submitted to the Central U.S. Registry (CUSR).

(ii) Access to NATO classified information may be permitted for citizens of NATO member nations, provided a NATO security clearance certificate is provided by their government and they have been briefed.

(9) *Subcontracting for NATO contracts.* The contractor will obtain prior written approval from the NATO contracting activity and a NATO FSCC must be issued prior to awarding the subcontract. The contractor will forward the request for approval through the CSA.

(10) *Preparing and marking NATO documents.* All classified documents created by a U.S. contractor will be portion-marked. Any portion extracted from a NATO document that is not portion marked, must be assigned the classification that is assigned to the NATO document.

(i) All U.S.-originated NATO classified documents will bear an assigned reference number and date on the first page. The reference numbers will be assigned as follows:

(A) The first element will be the abbreviation for the name of the contractor.

(B) The second element will be the abbreviation for the highest classification followed by a hyphen and the 4-digit sequence number for the document within that classification that has been generated for the applicable calendar year.

(C) The third element will be the year; *e.g.,* MM/NS–0013/17.

(ii) COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents will bear the reference number on each page and a copy number on the cover or first page.

(A) Copies of NATO documents will be serially numbered.

(B) Pages will be numbered.

(C) The first page, index, or table of contents will include a list, including page numbers, of all annexes and appendices.

(D) The total number of pages will be stated on the first page.

(E) All annexes or appendices will include the date of the original document and the purpose of the new text (addition or substitution) on the first page.

(iii) One of the following markings will be applied to NATO documents that contain ATOMAL information:

(A) ''This document contains U.S. ATOMIC Information (RESTRICTED DATA or FORMERLY RESTRICTED DATA) made available pursuant to the NATO Agreement for Cooperation Regarding ATOMIC Information, dated 18 June 1964, and will be safeguarded accordingly.''

(B) ''This document contains UK ATOMIC Information. This information is released to NATO including its military and civilian agencies and member states on condition that it will not be released by the recipient organization to any other organization or government or national of another country or member of any other organization without prior permission from H.M. Government in the United Kingdom.''

(iv) Working papers will be retained only until a final product is produced and in accordance with § 117.15(e)(3).

(11) *Classification guidance.* Classification guidance will be in the form of a NATO security aspects letter and a security requirements checklist for NATO contracts, or a Contract Security Classification Specification, or equivalent.

(i) If adequate classification guidance is not received, the contractor will contact the CSA for assistance.

(ii) NATO classified documents and NATO information in other documents will not be declassified or downgraded without the prior written consent of the originating activity.

(iii) Recommendations concerning the declassification or downgrading of NATO classified information will be forwarded to the CUSR.

(12) *Further distribution.* The contractor will not release or disclose NATO classified information to a third party or outside the contractor's facility for any purpose without the prior written approval of the contracting agency.

(13) *Storage of NATO documents.* NATO classified documents will be stored as prescribed for U.S. documents of an equivalent classification level, except as follows:

(i) NATO classified documents will not be comingled with other documents.

(ii) Combinations for containers used to store NATO classified information will be changed annually. The combination also will be changed when an individual with access to the container departs or no longer requires access to the container, and if the combination is suspected of being compromised.

(iii) When the combination is recorded it will be marked with the highest classification level of documents stored in the container as well as to indicate the level and type of NATO documents in the container. The combination record must be logged and controlled in the same manner as NATO classified documents.

(14) *International transmission.* The NATO has a registry system for the receipt and distribution of NATO documents within each NATO member nation. The central distribution point for the United States is the CUSR now located at 9301 Chapek Road, Building 1458, Fort Belvoir, Virginia 22060.

(i) The CUSR establishes sub registries at USG organizations for further distribution and control of NATO documents. Sub registries may establish control points at contractor facilities.

(ii) COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents will be transferred through the registry system. NATO CONFIDENTIAL documents provided as part of NATO infrastructure contracts will be transmitted via government channels in compliance with paragraph (d) in this section.

(15) *Hand carrying.* NATO SECRET and NATO CONFIDENTIAL documents may be hand carried across international borders if authorized by the GCA. The courier will be issued a NATO Courier Certificate by the CSA. When hand carrying is authorized, the documents will be delivered to a U.S. organization at NATO, which will transfer them to the intended NATO recipient.

(16) *Reproduction.* Reproductions of COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL information will be performed by the responsible Registry. The reproduction of NATO SECRET and CONFIDENTIAL documents may be authorized to meet contractual requirements unless reproduction is prohibited by the contracting entity. Copies of COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents will be serially numbered and controlled and accounted for in the same manner as the original.

(17) *Disposition.* (i) Generally, all NATO classified documents will be returned to the contracting activity that provided them on completion of the contract. Documents provided in connection with an invitation to bid also will be returned immediately if the bid is not accepted or submitted.

(ii) NATO classified documents may also be destroyed when permitted. COSMIC TOP SECRET and COSMIC TOP SECRET ATOMAL documents will be destroyed by the registry that provided the documents.

(A) Destruction certificates are required for all NATO classified documents except NATO CONFIDENTIAL.

(B) The destruction of COSMIC TOP SECRET, NATO SECRET, and all ATOMAL documents must be witnessed.

(18) *Accountability records.* Logs, receipts, and destruction certificates are required for NATO classified information. Records for NATO documents will be maintained separately from records of non-NATO documents (methods such as separate drawers of a container).

(i) COSMIC TOP SECRET and all ATOMAL documents will be recorded on logs maintained separately from other NATO logs and will be assigned unique serial control numbers.

(ii) Additionally, disclosure records bearing the name and signature of each person who has access are required for all COSMIC TOP SECRET, COSMIC TOP SECRET ATOMAL, and all other ATOMAL or NATO classified documents to which special access limitations have been applied.

(iii) Minimum identifying data on logs, receipts, and destruction certificates will include the NATO reference number, short title, date of the document, classification, and serial copy numbers. Logs will reflect the short title, unclassified subject, and distribution of the documents.

(iv) Receipts are required for all NATO classified documents except NATO CONFIDENTIAL.

(v) Inventories will be conducted annually of all COSMIC TOP SECRET, NATO SECRET, and ATOMAL documents.

(vi) Accountability records for ATOMAL documents will be retained for 10 years after transfer or destruction of the ATOMAL document. Destruction certificates will be retained for 10 years after destruction of the related ATOMAL documents.

(19) *Security violations and loss, compromise, or possible compromise.* The contractor will immediately report the loss, compromise, or suspected loss or compromise, as well as any other security violations involving NATO classified information to the CSA.

(20) *Extracting from NATO documents.* Permission to extract from a COSMIC TOP SECRET or ATOMAL document will be obtained from the CUSR.

(i) If extracts of NATO information are included in a U.S. document prepared for a non-NATO contract, the document will be marked with U.S. classification markings. The caveat, ''THIS DOCUMENT CONTAINS NATO (level of classification) INFORMATION'' also will be marked on the front cover or first page of the document. Additionally, each paragraph or portion containing the NATO information will be marked with the appropriate NATO classification, abbreviated in parentheses (*e.g.,* ''NS'' for NATO SECRET) preceding the portion or paragraph. Declassification and downgrading instructions shall indicate that the NATO information is exempt from declassification or downgrading without the prior consent of NATO, in the absence of other originator instructions, citing the reason ''Foreign Government Information.''

(ii) The declassification or downgrading of NATO information in a U.S. document requires the approval of the originating NATO activity. Requests will be submitted to the CUSR for NATO contracts, through the GCA for U.S. contracts, and through the CSA for non-NATO contracts awarded by a NATO member nation.

(21) *Release of U.S. information to NATO.* (i) Release of U.S. classified or export-controlled information to NATO requires an export authorization or other written disclosure authorization. When a document containing U.S. classified information is being prepared for NATO, the appropriate NATO classification markings will be applied to the document.

(A) Documents containing U.S. classified information and U.S. classified documents that are authorized for release to NATO will be marked on the cover or first page ''THIS DOCUMENT CONTAINS U.S. CLASSIFIED INFORMATION. THE INFORMATION IN THIS DOCUMENT HAS BEEN AUTHORIZED FOR RELEASE TO (cite the NATO organization) BY (cite the applicable license or other written authority).''

(B) The CSA will provide transmission instructions to the contractor. The material will be

addressed to a U.S. organization at NATO, which will then place the material into NATO security channels. The material will be accompanied by a letter to the U.S. organization that provides transfer instructions and assurances that the material has been authorized for release to NATO. The inner wrapper will be addressed to the intended NATO recipient.

(C) Material to be sent to NATO via mail will be routed through the U.S. Postal Service and U.S. military postal channels to the U.S. organization that will make the transfer.

(ii) A record will be maintained that identifies the originator and source of classified information that are used in the preparation of documents for release to NATO. The record will be provided with any request for release authorization.

(22) *Visits.* NATO visits will be handled in accordance with the requirements in paragraph (e) of this section. A NATO Certificate of Security Clearance will be included with the visit request.

(i) *NPLO and NATO industrial advisory group (NIAG) recurring visits.* NATO has established special procedures for recurring visits involving contractors, government departments and agencies, and NATO commands and agencies that are participating in a NPLO or NIAG contract or program. The NATO management office or agency responsible for the NPLO program will prepare a list of the government and contractor facilities participating in the program. For NIAG programs, the list will be prepared by the responsible NATO staff element. The list will be forwarded to the appropriate clearance agency of the participating nations, which will forward it to the participating contractor.

(ii) *Visitor record.* The contractor will maintain a record of NATO visits including those by U.S. personnel assigned to NATO. The records will be maintained for three years.

(h) *Security and export control violations involving foreign nationals.* Contractors will report any violation of administrative security procedures or export control regulations that would subject classified information to possible compromise by foreign visitors or foreign national employees to the applicable CSA.

(i) *Transfers of defense articles to the UK or AUS without a license or other written authorization.*—(1) *Treaties with AUS and UK.* Exemptions in ITAR parts 126.16 and 126.17 implement the Defense Trade Cooperation Treaty between the Government of the United States of America and the Government of the UK of Great Britain and Northern Ireland and the Defense Trade Cooperation Treaty between the Government of the United States of America and the Government of AUS, also known as the ''U.S.-UK Treaty'' and ''U.S.-AUS Treaty,'' respectively, referred to collectively in this rule as ''the Treaties.''

(i) The Treaties provide a comprehensive framework for exports and transfers to the UK or AUS of certain classified and unclassified defense articles without a license or other written authorization.

(ii) The ITAR part 126, supplement no. 1 identifies those defense articles and services that are not eligible for export via treaty exemptions.

(iii) This exemption applies to contractors registered with the DDTC and eligible to export defense articles.

(2) *Defense articles.* Defense articles fall under the scope of the Treaties when they are in support of:

(i) U.S. and UK or U.S. and AUS combined military or counter-terrorism operations.

(ii) U.S. and UK or U.S. and AUS cooperative security and defense research, development, production, and support programs.

(iii) Mutually agreed specific security and defense projects where the government of the UK or AUS is the end-user.

(iv) USG end-use.

(3) *Marking requirements.* Contractors are required to mark defense articles that fall under the scope of the treaty prior to transferring from the U.S. to the UK in accordance with the provisions of this paragraph. All other standard classification marking in accordance with § 117.14 also apply. When defense articles are returned from the UK or AUS to the United States, any defense articles marked as RESTRICTED in the manner shown in Table 4 purely for the purposes of the treaties will be considered to be unclassified and such marking will be removed.

TABLE 3 TO PARAGRAPH (i)(3) CLASSIFIED U.S. DEFENSE ARTICLE MARKINGS

UNCLASSIFIED: CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Treaty with:	Marking	Example (for SECRET classified defense articles)
Government of UK	//CLASSIFICATION LEVEL USML/REL GBR AND USA TREATY COMMUNITY//.	//SECRET USML//REL GBR AND USA TREATY COMMUNITY//''
Government of AUS	//CLASSIFICATION LEVEL USML/REL AUS AND USA TREATY COMMUNITY//.	//SECRET USML//REL AUS AND USA TREATY COMMUNITY//''

TABLE 4 TO PARAGRAPH (i)(3) UNCLASSIFIED U.S. DEFENSE ARTICLE MARKINGS

UNCLASSIFIED: CLASSIFICATION MARKINGS FOR ILLUSTRATION PURPOSES ONLY

Treaty with:	Marking
Government of UK	//RESTRICTED–USML//REL GBR AND USA TREATY COMMUNITY//
Government of AUS	//RESTRICTED–USML//REL AUS AND USA TREATY COMMUNITY//

(4) *Notice.* A notice will be included (*e.g.,* as part of the bill of lading) whenever defense articles are exported in accordance with the provisions of these treaties and the ITAR.

TABLE 5 TO PARAGRAPH (i)(4) NOTICE TEXT FOR EXPORTED DEFENSE ARTICLES

Notice text	These U.S. Munitions List commodities are authorized by the U.S. Government under the U.S. [AUS or UK, as applicable] Defense Trade Cooperation Treaty for export only to [AUS or UK, as applicable] for use in approved projects, programs or operations by members of the [AUS or UK, as applicable] Community. They may not be retransferred or re-exported or used outside of an approve project, program, or operation, either in their original form or after being incorporated into other end-items, without the prior written approval of the U.S. Department of State.

(5) *Labeling.* (i) Defense articles (other than technical data) will be individually labeled with the appropriate identification; or, where such labeling is impracticable (*e.g.,* propellants, chemicals), will be accompanied by documentation (such as contracts or invoices) clearly associating the defense articles with the appropriate markings.

(ii) Technical data (including data packages, technical papers, manuals, presentations, specifications, guides and reports), regardless of media or means of transmission (*i.e.,* physical, oral, or electronic), will be individually labeled with the appropriate identification detailed. Where such labeling is impracticable, the data will be accompanied by documentation (such as contracts or invoices) or oral notification clearly associating the technical data with the appropriate markings.

(iii) Defense services will be accompanied by documentation (*e.g.* contracts, invoices, shipping bills, or bills of lading clearly labeled with the appropriate identification).

(6) *Transfers.* (i) All defense articles that fall under the scope of the Treaties must be transferred from the U.S. point of embarkation through channels approved by both the United States and the UK or the United States and AUS, as applicable.

(ii) For transfers of defense articles as freight, the contractor will prepare a transportation plan. For transfer of classified U.S. defense articles, a freight forwarder must have a valid entity eligibility determination and a classified information storage capability at the appropriate level. For unclassified U.S. defense articles transferred as freight, a freight forwarder is not required to be cleared.

(7) *Records.* Contractors will maintain records of exports, transfers, re-exports, or re-transfers of defense articles subject to the Treaties for a minimum of five years. The contractor will make records available to the CSA upon request. In accordance with the ITAR parts 126.16 and 126.17 the records will contain:

(i) Port of entry or exit.

(ii) Date and time of export or import.

(iii) Method of export or import.

(iv) Commodity code and description of the commodity, including technical data.

(v) Value of export.

(vi) Justification for export under the Treaties.

(vii) End-user or end-use.

(viii) Identification of all U.S. and foreign parties to the transaction.

(ix) How export was marked.

(x) Security classification of the export.

(xi) All written correspondence with the USG on the export.

(xii) All information relating to political contributions, fees, or commissions furnished or obtained, offered, solicited, or agreed upon, as outlined in the ITAR parts 126.16(m) or 126.17(m).

(xiii) Purchase order, contract, or letter of intent.

(xiv) Technical data actually exported.

(xv) The internal transaction number for the electronic export information filing in the automated export system.

(xvi) All shipping documentation (including, but not limited to, the airway bill, bill of lading, packing list, delivery verification, and invoice).

(xvii) Statement of registration (Department of State Form DS–2032 (available at: *https://www.pmddtc.state.gov/sys_attachment.do?sysparm_referring_url=tear_off&view=true&sys_id=dabc05f6db6be344529d368d7c961984*)).

§ 117.20 Critical Nuclear Weapon Design Information (CNWDI).

(a) *General.* This section contains the special requirements for protection of CNDWI. The sensitivity of DoD CNWDI is such that access shall be granted to the absolute minimum number of employees who require it for the accomplishment of assigned responsibilities on a classified contract. Because of the importance of such information, special requirements have been established for its control. DoDI 5210.02, ''Access to and Dissemination of Restricted Data and Formerly Restricted Data'' (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/521002p.pdf?ver=2019-01-14-072742-700*) establishes these controls in the DoD.

(b) *Briefings.* Prior to having access to CNWDI, employees will be briefed on its sensitivity by the FSO or his or her alternate. The FSO will be initially briefed by a USG representative.

(1) The briefing will include:

(i) The definition of CNWDI.

(ii) A reminder of the extreme sensitivity of the information.

(iii) An explanation of the individual's continuing responsibility for properly safeguarding CNWDI and for ensuring that dissemination is strictly limited to other personnel who have been authorized for access and have a need-to-know for the particular information.

(2) The briefing will also be tailored to cover any special local requirements. Upon termination of access to CNWDI, the employee will be given an oral debriefing.

(c) *Markings.* In addition to any other required markings, CNWDI material will be clearly marked in accordance with DoDI 5210.02. At a minimum, CNWDI documents will show such markings on the cover or first page. Portions of documents that contain CNWDI will be marked with an (N) or (CNWDI) following the classification of the portion; for example, TS (RD)(N) or TS(RD)(CNWDI).

(d) *Subcontractors.* Contractors will not disclose CNWDI to subcontractors without the prior written approval of the GCA. This approval may be included in a contract security classification specification, or equivalent, other contract-related document, or by separate correspondence.

(e) *Transmission outside the facility.* Transmission of CNWDI outside the contractor's facility is authorized only to the GCA, or to a subcontractor as described in paragraph (d) of this section. Any other transmission must be approved by the GCA.

(1) Prior to transmission to another cleared facility, the contractor will verify from the CSA that the facility has been authorized access to CNWDI. When CNWDI is transmitted to another facility, the inner wrapping will be addressed to the personal attention of the FSO or his or her alternate, and in addition to any other prescribed markings, the inner wrapping will be marked: ''Critical Nuclear Weapon Design Information-DoD Instruction 5210.02 Applies.''

(2) The same marking will be used on the inner wrapping of transmissions addressed to the GCA or other USG.

(f) *Records.* Contractors will annotate CNWDI access in the CSA-designated database for all employees who have been authorized access to CNWDI.

(g) *Nuclear weapon data.* Some nuclear weapon data is divided into Sigma categories, the protection of which is prescribed by DOE Order 452.8 (available at: *https://www.directives.doe.gov/directives-documents/400-series/0452.8-border/@@images/file*). However, certain nuclear weapon data has been re-categorized as CNWDI and is protected as described in this section.

§ 117.21 COMSEC.

(a) *General.* The procedures in this section pertaining to classified COMSEC information will apply to contractors when the contractor:

(1) Requires the use of COMSEC systems in the performance of a contract.

(2) Is required to install, maintain, or operate COMSEC equipment for the USG.

(3) Is required to accomplish research, development, or production of COMSEC systems, COMSEC equipment, or related COMSEC material.

(b) *Instructions.* Specific requirements for the management and safeguarding of COMSEC material in industry are established in the COMSEC material control and operating procedures provided to the account manager of each industrial COMSEC account by the agency central office of record (COR) responsible for establishing the account. Such procedures that are above the baseline requirements detailed in the other sections of this rule will be contractually mandated.

(c) *Clearance and access requirements.* (1) Before a COMSEC account can be established and a contractor may receive or possess COMSEC material accountable to a COR, individuals occupying the positions of FSO, COMSEC account manager, and alternate COMSEC account manager must have a final PCL appropriate for the material to be held in the account.

(i) COMSEC account managers and alternate COMSEC account managers having access to operational TOP SECRET keying material marked as CRYPTO must have a final TOP SECRET security clearance based upon a current investigation of a scope that meets or exceeds that necessary for the access required.

(ii) This requirement does not apply to contractors using only data transfer devices and seed key.

(2) Before disclosure of COMSEC information to a contractor, GCAs must first verify with the CSA that appropriate COMSEC procedures are in place at the contractor facility. If procedures are not in place, the GCA will provide a written request and justification to the CSA to establish COMSEC procedures and a COMSEC account, if appropriate, at the facility and to conduct the initial COMSEC or cryptographic access briefings for the FSO and COMSEC account personnel.

(3) Access to COMSEC information by a contractor requires a final entity eligibility determination and a USG-issued final PCL at the appropriate level; however, an Interim TOP SECRET entity eligibility determination or PCL is valid for access to COMSEC at the SECRET and CONFIDENTIAL levels.

(4) If a COMSEC account will be required, the Contract Security Classification Specification, or equivalent, will contain a statement regarding the establishment of a COMSEC account as appropriate.

(d) *Establishing a COMSEC account.* (1) When COMSEC material that is accountable to a COR is to be provided, acquired, or produced under a contract, the contracting officer will inform the contractor that a COMSEC account must be established. The contractor will forward the names of U.S. citizen employees who will serve as the COMSEC account manager and alternate COMSEC account manager to the CSA. The CSA will forward the names of the FSO, COMSEC account manager, and alternate COMSEC account manager, along with a contractual requirement for the establishment of a COMSEC account (using DD Form 254 or equivalent) to the appropriate COR, with a copy to the GCA, indicating that the persons have been cleared and COMSEC has been briefed.

(2) The COR will then establish the COMSEC account and notify the CSA that the account has been established.

(3) An individual may be appointed as the COMSEC account manager or alternate COMSEC account manager for more than one account only when approved by each COR concerned.

(e) *COMSEC briefing and debriefing.* (1) All contractor employees who require access to classified COMSEC information in the performance of their duties will be briefed before access is granted. Depending on the nature of COMSEC access required, either a COMSEC briefing or a cryptographic access briefing will be given. The FSO, the COMSEC account manager, and the alternate COMSEC account manager will be briefed by a USG representative or their designee. Other contractor employees will be briefed by the FSO, the COMSEC account personnel, or other individual designated by the FSO. The purpose of the briefing is to ensure that the contractor understands:

(i) The unique nature of COMSEC information and its unusual sensitivity.

(ii) The special security requirements for the handling and protection of COMSEC information.

(iii) The penalties prescribed in 18 U.S.C. 793, 794, and 798 for disclosure of COMSEC information.

(2) COMSEC debriefings are not required.

(3) The contractor will maintain a record of all COMSEC briefings as specified by the appropriate COR.

(f) *U.S. classified cryptographic information access briefing and debriefing requirements.* (1) U.S. classified cryptographic information does not include seed key or controlled cryptographic items.

(2) A contractor's employee may be granted access to U.S. classified cryptographic information only if the employee:

(i) Is a U.S. citizen.

(ii) Has a final USG-issued eligibility determination appropriate to the classification of the U.S. cryptographic information to be accessed.

(iii) Has a valid need-to-know to perform duties for, or on behalf of, the USG.

(iv) Receives a security briefing appropriate to the U.S. Classified Cryptographic Information to be accessed.

(v) Acknowledges the granting of access to classified information by executing Section I of Secretary of Defense (SD) Form 572, ''Cryptographic Access Certification and Termination'' (available at: *https://www.esd.whs.mil/Portals/54/Documents/DD/forms/sd/sd0572.pdf*).

(vi) Where so directed by a USG department or agency head, acknowledges the possibility of being subject to a CI scope polygraph examination that will be administered in accordance with department or agency directives and applicable law.

(3) An employee granted access to cryptographic information will be debriefed and execute Section II of the SD 572 not later than 90 days from the date access is no longer required.

(4) The contractor will maintain the SD 572 for a minimum of five years following the debriefing.

(5) Cryptographic access briefings must fully meet the requirements of paragraph (e) of this section.

(g) *Destruction and disposition of COMSEC material.* The appropriate GCA representative, *e.g.,* the contracting officer representative, will provide directions to the contractor when accountable COMSEC material is to be destroyed. These directions may be provided in superseding editions of publications or by specific instructions.

(h) *Subcontracting COMSEC work.* Subcontracts requiring the disclosure of classified COMSEC information will be awarded only upon the written approval of the GCA.

(i) *Unsolicited proposals.* Any unsolicited proposal for a COMSEC system, equipment, development, or study that may be submitted by a contractor to a USG agency will be forwarded to the Deputy National Manager for National Security Systems for review and follow up action at: Deputy National Manager for National Security Systems, NSA, Fort George G. Meade, MD 20755–6000.

§ 117.22 DHS CCIPP.

(a) *General.* DHS will coordinate with other USG agencies that have an equity with a private sector entity and the CCIPP in accordance with § 117.6(f).

(b) *Authority.* (1) The Secretary of Homeland Security has the authority to determine the eligibility for personnel security clearances and to administer the sharing of relevant classified NSI with certain private sectors or non-federal partners for the purpose of furthering cybersecurity information sharing among critical infrastructure partners pursuant to E.O. 13691.

(2) DHS provides security oversight and assumes security responsibilities similar to those of an FSO, unless otherwise provided in this section. Participating entities will cooperate with DHS security officials to ensure the entity is in compliance with requirements in this rule.

§ 117.23 Supplement to this rule: Security Requirements for Alternative Compensatory Control Measures (ACCM), Special Access Programs (SAPs), Sensitive Compartmented Information (SCI), Restricted Data (RD), Formerly Restricted Data (FRD), Transclassified Foreign Nuclear Information (TFNI), and NNPI.

(a) *General.* Given the sensitive nature of Alternative Compensatory Control Measures (ACCM), SAPs, SCI, RD, FRD, TFNI, and NNPI, the security requirements prescribed in this section exceed baseline standards for this rule and must be applied, as applicable, through specific contract requirements.

(1) *Compliance.* The contractor will comply with the security measures reflected in this section and other documents specifically referenced, when applied by the GCA or designee as part of a contract. Acceptance of the contract security measures is a prerequisite to any negotiations leading to program participation and an area accreditation (*e.g.,* an SCI facility or SAP facility accreditation).

(2) *CSA-imposed higher standards.* In some cases, security or sensitive factors of a CSA-created program may require security measures that exceed the standards of this section. In such cases, the CSA-imposed higher standards specifically detailed in the contract or conveyed through other applicable directives will be binding on USG and contractor participants. In cases of doubt over the specific provisions, the contractor should consult the program security officer and the contracting officer before taking any action or expending program-related funds. In cases of extreme emergencies requiring immediate attention, the action taken should protect the USG's interest and the security of the program from loss or compromise.

(3) *Waivers.* Every effort will be made to avoid waivers to established standards unless they are in the best interest of the USG. In those cases where waivers are deemed necessary, a request will be submitted in accordance with the procedures established by the CSA.

(b) *Intelligence information.* National intelligence is under the jurisdiction and control of the DNI, who establishes security policy for the protection of national intelligence and intelligence sources, methods, and activities. In addition to the guidance in this rule, contractors will follow Intelligence Community directives, policy guidance, standards, and specifications for the protection of classified national intelligence and SCI.

(c) *ACCM.* Contractors may participate in ACCMs, or be directed to participate, only when such access and the associated security plan are identified in DD Form 254 or equivalent. Care must be taken to ensure identification of the security plan does not disclose ACCM-protected data.

(1) *ACCM contracts.* DoD contractors will implement the security requirements for ACCMs, when established by contract, in accordance with applicable statutes, E.O.s, CSA directives, instructions, manuals, regulations, standards, and memorandums.

(2) *Non-DoD with ACCMs.* Contractors performing on ACCM contracts issued by other than DoD GCAs will implement ACCM protection requirements imposed in their contracts.

(d) *SAPs.*—(1) *DoD SAP contracts.* Contractors will implement the security requirements for SAPs codified in SAP-related policy, when established by contract. These documents include, but are not limited to, statutes, E.O.s, CSA directives, instructions, manuals, regulations, standards, memorandums, and other SAP security related policy documents.

(2) *Non-DoD SAPs.* Contractors performing on SAP contracts issued by non-DoD GCAs will implement SAP protection requirements imposed in their contracts. These requirements may be from, but are not limited to, statutes, E.O.s, CSA directives, instructions, manuals, regulations, standards, memorandums, and other SAP security related policy documents.

(e) *RD, FRD, and TFNI.*—(1) *General.* This section describes some of the requirements for nuclear-related information designated RD, FRD, or TFNI in accordance with the AEA and 10 CFR part 1045. 10 CFR part 1045 contains the full requirements for classification and declassification of RD, FRD, and TFNI. Information on safeguarding of RD by access permittees is contained in 10 CFR part 1016. For RD that is NNPI, the additional provisions of paragraph (f) of this section apply.

(i) The DOE is the sole authority for establishing requirements for classifying, accessing, handling, securing, and protecting RD. The DOE and the DoD share authority for the requirements for FRD. The DOE and ODNI share authority for establishing requirements for TFNI.

(ii) RD, FRD, and TFNI categories are distinguished from the NSI category, which is governed in accordance with E.O. 13526.

(A) RD, FRD, and TFNI have unique marking requirements and are not subject to automatic declassification. In addition, RD and FRD have special restrictions regarding foreign release.

(B) It is necessary to differentiate between the handling of this information and NSI because of its direct relationship to our nation's nuclear deterrent.

(iii) Some access requirements for RD and FRD exceed the requirements for NSI. Due to the unique national security implications of RD and FRD, and to facilitate maintaining consistency of codified requirement, they are not repeated in the baseline of this rule, but may be applied through specific contract requirements.

(iv) When RD is transclassified as TFNI, it is safeguarded as NSI. Such information will be labeled as TFNI. The label TFNI will be included on

documents to indicate it is exempt from automatic declassification as specified in 10 CFR part 1045, the AEA, E.O. 13526, and 32 CFR part 2001.

(2) *Unauthorized disclosures.* Contractors will report all unauthorized disclosures involving RD, FRD and TFNI information to the CSA.

(3) *International requirements.* The AEA provides for a program of international cooperation to promote common defense and security and to make available to cooperating nations the benefits of peaceful applications of atomic energy as widely as expanding technology and considerations of the common defense and security will permit.

(i) Information controlled in accordance with the AEA, RD, and FRD may be shared with another nation only under the terms of an agreement for cooperation. The disclosure by a contractor of RD and FRD will not be permitted until an agreement is signed by the United States and participating governments, and disclosure guidance and security arrangements are established.

(ii) RD and FRD will not be transmitted to a foreign national or regional defense organization unless such action is approved and undertaken under an agreement for cooperation between the United States and the cooperating entity and supporting statutory determinations, as prescribed in the AEA.

(4) *Personnel security clearance and access.* Only the DOE, the NRC, the DoD, and the National Aeronautics and Space Agency can grant access to RD and FRD that is under their cognizance. Access to RD and FRD must be granted in accordance with the AEA. Baseline requirements for access to RD and FRD are codified in specific DoD, DOE, NRC, and the National Aeronautics and Space Agency directives and regulations. In addition, need-to-know and other restrictions on access apply.

(5) *Classification and declassification.* (i) All persons with access to RD and FRD must receive initial and periodic refresher training as required under § 1045.120 10 CFR. The training must include the following information:

(A) What information is potentially RD and FRD.

(B) Matter that potentially contains RD or FRD must be reviewed by an RD derivative classifier to determine whether it is RD or FRD.

(C) The DOE must review matter that potentially contains RD or TFNI for public release and DOE or DoD must review matter that potentially contains FRD for public release.

(D) RD derivative classification authority is required to classify or upgrade matter containing RD or FRD, or to downgrade the level of matter containing RD or FRD.

(E) Only a person trained in accordance with § 1045.120 10 CFR may classify matter containing TFNI.

(F) Matter containing RD, FRD, and TFNI is not automatically declassified and only DOE-authorized persons may downgrade the category or declassify matter marked as containing RD. Only DOE or DoD authorized persons may downgrade the category or declassify matter marked as containing FRD.

(G) How to submit a challenge if they believe RD, FRD, or TFNI information (*e.g.,* a guide topic) or matter containing RD, FRD, or TFNI is not properly classified.

(H) Access requirements for matter marked as containing RD or FRD.

(ii) All persons with access to TFNI must receive initial and periodic refresher training as required under § 1045.120 10 CFR. This training may be combined with the training for access to RD and FRD. The training must include the following information:

(A) What information is potentially TFNI.

(B) Only a person with appropriate training may determine if matter contains TFNI.

(C) Marking requirements for matter containing TFNI.

(D) Matter containing TFNI is not automatically declassified and only DOE authorized persons may downgrade the category or declassify matter marked as containing TFNI.

(E) How to submit a challenge if they believe TFNI information (*e.g.,* a guide topic) or matter containing TFNI is not properly classified.

(iii) Persons with access to RD, FRD, or TFNI must submit matter that potentially contains RD or FRD to an RD derivative classifier for review. If matter potentially contains TFNI, it must be submitted to a person trained to make TFNI determinations. Matter potentially containing RD, FRD, or TFNI must be reviewed, even if the potential RD, FRD, or TFNI is derived from the open literature. Prior to review, the matter must be marked as a working paper under 10 CFR 1045.140(c). If the matter is intended for pubic release and potentially contains RD or TFNI, it must be submitted to the DOE for review. If the matter is intended for public release and contains FRD, it must be submitted to the DOE or the DoD.

(iv) Only RD derivative classifiers may classify matter containing RD or FRD. RD derivative classifiers must receive initial training and refresher training every two years as required under 10 CFR 1045.120. The training must include the content for persons with access to RD and FRD, along with the following:

(A) The use of classification guides, classification bulletins, and portion-marked source documents to classify matter containing RD and FRD.

(B) What to do if applicable classification guidance is not available.

(C) Limitations on an RD derivative classifier's authority to remove RD or FRD portions from matter.

(D) Marking requirements for matter containing RD and FRD.

(v) Only persons with appropriate training may review matter to determine if it contains TFNI. Training must be completed prior to making determinations and every two years after. The training must include the content for persons with access to TFNI and the following:

(A) The markings applied to matter containing TFNI.

(B) Limitations on their authority to remove TFNI portions from matter.

(C) Only DOE authorized persons may determine that classified matter no longer contains TFNI.

(D) Only DOE-authorized persons may declassify matter marked as containing TFNI.

(E) The DOE must review matter that potentially contains TFNI for public release.

(vi) RD derivative classifiers must use approved classification guides, classification bulletins, or portion-marked source documents as the basis for classifying matter containing RD and FRD.

(vii) Persons trained to make TFNI determinations must use approved TFNI guidelines, classification guides, classification bulletins, or portion-marked source documents as the basis for classifying or upgrade matter containing TFNI.

(6) *Marking matter containing RD, FRD, and TFNI.* The front page of matter containing RD or FRD must have the highest classification level of the information on the top and bottom of the first page, the RD or FRD admonishment, the subject or title marking, and the classification authority block. Matter containing TFNI must include the TFNI identifier on each page unless the matter also contains RD or FRD, in which case the RD or FRD takes precedence.

(i) Documents classified as RD or FRD must also include a Classification Authority Block with the RD derivative classifier's name and position, title, or unique identifier and the classification guide or source document (by title and

date) used to classify the document. No declassification date or event may be placed on a document containing RD, FRD, or TFNI. If a document containing RD, FRD, or TFNI also contains NSI, ''N/A to RD/FRD/TFNI'' (as appropriate) must be placed on the ''Declassify On:'' line.

(ii) Each interior page of matter containing RD or FRD must be clearly marked at the top and bottom with the overall classification level and category of the matter or the overall classification level and category of the page, whichever is preferred. The abbreviations ''RD'' or ''FRD'' may be used in conjunction with the matter classification (*e.g.,* SECRET//RD, CONFIDENTIAL//FRD).

TABLE 1 TO PARAGRAPH (e)(6)(ii) RD AND FRD ADMONISHMENT MARKINGS

Document containing	Admonishment that must be included on the front page of the document
RD	''RESTRICTED DATA This document contains RESTRICTED DATA as defined in the Atomic Energy Act of 1954. Unauthorized disclosure is subject to administrative and criminal sanctions.''
FRD	''FORMERLY RESTRICTED DATA Unauthorized disclosure subject to administrative and criminal sanctions. Handle as Restricted Data in foreign dissemination. Section 144b, AEA 1954.''

(iii) Documents classified as RD or FRD must also include a Classification Authority Block with the RD derivative classifier's name and position, title, or unique identifier and the classification guide or source document (by title and date) used to classify the document.

(iv) Other than the required subject or title markings, portion marking is permitted, but not required, for matter containing RD or FRD. Each agency that generates matter containing RD or FRD determines the policy for portion-marking matter generated within the agency. If matter containing RD or FRD is portion-marked, each portion containing RD or FRD must be marked with the level and category of the information in the portion (*e.g.,* SRD, CFRD, S//RD, C//FRD).

(v) Additional information and requirements are in 10 CFR 1045.140. Requests for additional information about the classification and declassification of RD, FRD, and TFNI can be directed to Agency RD Management Officials or the DOE Office of Classification at *outreach@hq.doe.gov* or at (301) 903–7567.

(7) *Declassification.* (i) No date or event for automatic declassification ever applies to RD, FRD, or TFNI documents, even if they contain classified NSI. RD, FRD, or TFNI documents remain classified until a positive action by a designated DOE official (for RD, FRD, or TFNI) or an appropriate DoD official (for FRD) is taken to declassify them.

(ii) RD derivative classifiers may remove RD or FRD from portion-marked source matter if the resulting matter is not for public release. RD derivative classifiers cannot declassify matter marked as containing RD, FRD, and TFNI. Matter that potentially contains RD or TFNI must be sent to designated individuals in the DOE and those containing FRD must be sent to designated individuals in the DoD for declassification or removal of the RD, FRD, or TFNI prior to public release.

(iii) Matter containing TFNI is excluded from the automatic declassification provisions of E.O. 13526 until the TFNI designation is properly removed by the DOE. When the DOE determines that a TFNI designation may be removed, any remaining classified information must be referred to the appropriate agency.

(iv) Any matter marked as or that potentially contains RD, FRD, or TFNI within a document intended for public release that contains RD or FRD subject area indicators must be reviewed by the appropriate DOE organization.

(8) *Challenges to RD, FRD, and TFNI.* A contractor employee who believes RD, FRD, or TFNI is classified improperly or unnecessarily may challenge that classification following the procedures established by the GCA. They may also send challenges directly to the Director, Office of Classification, AU–60/ Germantown Building; U.S. Department of Energy; 1000 Independence Avenue SW, Washington, DC 20585, at any time. Under no circumstance is an employee subject to retribution for challenging the classification status of RD, FRD, or TFNI.

(9) *Commingling.* Commingling of RD, FRD, and TFNI with NSI in the same document should be avoided to the greatest degree possible. When mixing this information cannot be avoided, the marking requirements in 10 CFR part 1045, section 140(f) and declassification requirements of 10 CFR part 1045, section 155 apply.

(10) *Protection of RD and FRD.* Most of the protection requirements for RD and FRD are similar to NSI and are based on the classification level. However, there are some protection requirements for certain RD information that may be applied through specific contract requirements by the GCA. These range from distribution limitations through the limitation of access to specifically authorized individuals to specific storage requirements, including the requirement for IDSs, and additional accountability records.

(i) Any DOE contractor that violates a classified information security requirement may be subject to a civil penalty under the provisions of 10 CFR part 824.

(ii) Certification is required for individuals authorized access to specific Sigma categories, as appropriate. Address questions regarding these requirements to *DOE's National Nuclear Security Administration, Office of Defense Programs.*

(iii) Storage and distribution requirements are determined by the classification level, category, and Sigma category. Sigma designation is not a requirement for all RD documents. Storage and distribution requirements will be dependent only on classification level and category.

(11) *Accountability.* In addition to TOP SECRET information, some SECRET RD information is considered accountable (*e.g.,* specific Sigma 14 matter). Each nuclear weapon data control point will keep a record of transactions involving Secret nuclear weapon data documents under its jurisdiction including origination, receipt, transmission, current custodian, reproduction, change of classification, declassification, and destruction.

(12) *Cybersecurity.* Classified databases, systems, and networks containing RD and FRD are protected under the requirements developed and distributed by the DOE Office of the Chief Information Officer.

(f) *NNPI.* NNPI is information associated with the Naval Nuclear Propulsion Program and is governed by Office of the Chief of Naval Operations

Instruction (OPNAVINST) N9210.3, ''Safeguarding of Naval Nuclear Propulsion Information'' (available at: *https://www.secnav.navy.mil/doni/Directives/09000%20General%20Ship%20Design%20and%20Support/09-200%20Propulsion%20Plants%20Support/N9210.3%20(Unclas%20Portion).pdf*). Naval Reactors, a joint DOE/Department of Navy organization established under 50 U.S.C. 2406 and 2511, is responsible for the protection of this information. All contracts which grant access to NNPI must require compliance with the specific safeguarding requirements contained in OPNAVINST N9210.3. All waivers or deviations involving security requirements protecting NNPI require Naval Reactors' concurrence. Classified NNPI may not be processed on any contractor information system unless approved by the cognizant authorizing authority with concurrence from Naval Reactors.

§ 117.24 Cognizant Security Office information.

(a) *DoD.* Refer to the DCSA website (*https://www.dcsa.mil*) for a listing of office locations and areas of responsibility and for information on verification of facility clearances and safeguarding. In those cases where the cleared facility is located on a DoD installation the applicable DCSA field office can advise if the installation commander is providing security oversight.

TABLE 1 TO PARAGRAPH (a) DOD COGNIZANT SECURITY OFFICE

Designation	Office name	Mailing address	Telephone No.
Headquarters, CSO	Defense Counterintelligence and Security Agency.	27130 Telegraph Rd., Quantico, VA 22134.	(888) 282–7682

(b) *DOE.*

TABLE 2 TO PARAGRAPH (b) DOE COGNIZANT SECURITY OFFICES

Designation	Office name	Mailing address	Telephone No.
Headquarters	Headquarters Office of Security Operations (AU–40).	19901 Germantown Road, Germantown, MD 20874.	(301) 903–2177
CSO, Clearance Agency, Central Verification Activity, Adjudicative Authority, and PCL and FCL databases.	DOE/National Nuclear Security Administration Office of Personnel and Facility Clearances and Classifications.	Pennsylvania & H Street, Kirtland Air Force Base, Albuquerque, NM 87116.	(505) 845–4154
CSO	U.S. Department of Energy, Idaho Operations Office.	850 Energy Drive, Idaho Falls, ID 83401.	(208) 526–2216

TABLE 3 TO PARAGRAPH (b) DOE COGNIZANT SECURITY OFFICES CONTINUED

Designation	Office name	Mailing address	Telephone No.
CSO, Naval Nuclear Propulsion Information.	Director, Naval Reactors	NA–30, 1240 Isaac Hull Ave., SE., Washington Navy Yard, DC 20376.	(202) 781–6297
CSO	U.S. Department of Energy, Office of Science Consolidated Service Center.	200 Administration Road, P.O. Box 2001, Oak Ridge, TN 37830.	(865) 576–2140
CSO	U.S. Department of Energy, Pacific Northwest Site Office.	902 Battelle Boulevard, Richland, WA 99354.	(888) 375–7665
CSO	U.S. Department of Energy, Richland Operations Office.	825 Jadwin Avenue, P.O. Box 550, Richland, WA 99352.	(509) 376–7411
CSO	U.S. Department of Energy, Savannah River Operations Office.	Road 1A, Aiken, SC 29801	(803) 725–6211

(c) *NRC.*

TABLE 4 TO PARAGRAPH (c) NRC COGNIZANT SECURITY OFFICES

Designation	Mailing address	Telephone No.
CSO, Adjudicative Authority, PCL and FCL databases, and Industrial Security Program.	U.S. Nuclear Regulatory Commission, ATTN: Director of Facilities and Security, Washington, DC 20555.	(301) 415–8080
CSO, FCL Database and Industrial Security Program for Licensees.	U.S. Nuclear Regulatory Commission, ATTN: Information Security Branch, 11555 Rockville Pike, Rockville, MD 20853.	(301) 415–7048
Clearance Agency	U.S. Nuclear Regulatory Commission, ATTN: Director of Facilities and Security Personnel Security, 11545 Rockville Pike, Rockville, MD 20853.	(301) 415–8080
Central Verification Agency	U.S. Nuclear Regulatory Commission, ATTN: Director of Security Facilities Security, 11545 Rockville Pike, Rockville, MD 20853.	(301) 415–8080

(d) *DHS.*

TABLE 6 TO PARAGRAPH (d) DHS COGNIZANT SECURITY OFFICE

Designation	Mailing address	Telephone No.
CSO	DHS Cognizant Security Office, ATTN: Chief Security Officer, 245 Murray Lane, M/S 0120–3, Washington, DC 20528.	(202) 447–5424; (202) 447–5345

Dated: December 11, 2020.

Patricia L. Toppings,

OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2020–27698 Filed 12–18–20; 8:45 am]

BILLING CODE 5001–06–P