Billing Code 7515-01U

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION

Information Security Oversight Office

32 CFR Part 2004

[FDMS No. NARA-16-0006; Agency No. NARA-2017-017]

RIN 3095-AB79

National Industrial Security Program

AGENCY: Information Security Oversight Office, National Archives and Records Administration (NARA).

ACTION: Proposed rule.

SUMMARY: The Information Security Oversight Office (ISOO) of the National Archives and Records Administration (NARA), proposes to revise the National Industrial Security Program (NISP) Directive. The NISP safeguards classified information the Federal Government or foreign governments release to contractors, licensees, grantees, and certificate holders. This proposed revision adds provisions incorporating executive branch insider threat policy and minimum standards, identifies the Office of the Director of National Intelligence (ODNI) and the Department of Homeland Security (DHS) as new cognizant security agencies (CSAs), and adds responsibilities for all CSAs and non-CSA departments and agencies (to reflect oversight functions that are already detailed for private sector entities in the National Industrial Security Program Operating Manual (NISPOM)). The proposed revisions also make other administrative changes to be consistent with recent revisions to the NISPOM and with updated regulatory language and style.

DATES: Submit comments by [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by RIN 3095-AB79, by any of the following methods:

- *Federal eRulemaking Portal:* http://www.regulations.gov. Follow the instructions for submitting comments.
- *E-mail:* Regulation_comments@nara.gov. Include RIN 3095-AB79 in the subject line of the message.
- *Mail* (for paper, disk, or CD-ROM submissions. Include RIN 3095-AB79 on the submission): Regulations Comments Desk (External Policy Program, Strategy and Performance Division (SP)); Suite 4100; National Archives and Records Administration; 8601 Adelphi Road; College Park, MD 20740-6001
- *Hand delivery or courier:* Deliver comments to the front desk at the address above.

Instructions: You must include on all submissions the Regulatory Information Number (RIN) for this rulemaking (RIN 3095-AB79) and NARA's name. We may publish any comments we receive without changes, including any personal information you provide.

FOR FURTHER INFORMATION CONTACT: For information about this regulation and the regulatory process, contact Kimberly Keravuori, External Policy Program Manager, by email at regulation_comments@nara.gov, or by telephone at 301.837.3151. For information about the NISP and the requirements in this regulation, contact William A. Cira, Acting Director, ISOO, by telephone at 202-357-5323.

SUPPLEMENTARY INFORMATION: We have coordinated and vetted the proposed revisions through the CSAs listed in Executive Order (E. O.) 12829, National Industrial Security

Program (January 6, 1993 (58 FR 3479)), as amended by E.O. 12885 (December 14, 1993 (58 FR 65863): Department of Defense, Department of Energy, Nuclear Regulatory Commission, Office of the Director of National Intelligence, and Department of Homeland Security. We have also coordinated this with the other executive branch agencies that are members of the National Industrial Security Program Policy Advisory Committee (NISPPAC) or that release classified information to contractors, licensees, grantees, or certificate holders, and with the industry members of the NISPPAC. The proposed revisions do not change requirements for industry (which are contained in the NISPOM), but instead clarify agency responsibilities.

Background

The NISP is the Federal Government's single, integrated industrial security program. E. O. 12829 (amended in 1993) established the NISP to safeguard classified information in industry and preserve the nation's economic and technological interests. The President issued E.O. 13691, Promoting Private Sector Cybersecurity Information Sharing (February 13, 2015 (80 FR 9347)), and E.O. 13708, Continuance or Reestablishment of Certain Federal Advisory Committees (September 30, 2015 (80 FR 60271)), which further amended E.O. 12829.

E.O. 12829, sec. 102(b), delegated oversight of the NISP to the Director of NARA's Information Security Oversight Office (ISOO). As part of ISOO's responsibilities under E.O. 12829, it is authorized to issue such directives as necessary to implement the E.O., which are binding on agencies. In 2006, ISOO issued, and periodically updates, this regulation, which functions as one of those directives.

This regulation establishes uniform standards throughout the Program, and helps agencies implement requirements in E.O. 12829, as amended (collectively referred to as "E.O. 12829"). This revision also establishes agency responsibilities for implementing the insider threat

provisions of E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (October 7, 2011 (76 FR 63811)) within the NISP. However, the regulation does not stand alone; users should refer concurrently to the underlying executive orders for guidance.

Nothing in this regulation supersedes the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011, *et seq.*); the authority of the Director of National Intelligence (or any intelligence community element) under the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub.L. 108-458), the National Security Act of 1947 (50 U.S.C. 401, *et seq.*), as amended, and E.O. 12333 (December 4, 1981), as amended by E.O. 13355, Strengthened Management of the Intelligence Community (August 27, 2004) and E.O. 13470, Further Amendments to Executive Order 12333 (July 30, 2008); or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under E.O. 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities (August 18, 2010), or by E. O. 13284, Amendment of Executive Orders, and Other Actions, in Connection with the Establishment of the Department of Homeland Security, (January 23, 2003).

Revision process and proposed changes

This proposed rule reflects a national level policy framework that should not change existing practices and procedures for any of the affected agencies or for entities in any significant way. A working group comprised of NISP CSA representatives, ISOO staff, the Department of Defense's (DoD) Defense Security Service (DSS), and the Central Intelligence Agency, drafted this proposed rule.

We initiated the proposed revisions in 2013 to incorporate new insider threat program requirements as a result of E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 2011, and the associated National Insider Threat Policy and Minimum Standards from the White House in November 2012. The national insider threat policy directs that the Government apply insider threat provisions to private sector entities that access classified information, which the executive branch accomplishes through the National Industrial Security Program Operating Manual (NISPOM), issued by the NISP Executive Agent, DoD. The NISPOM also provides private sector entities that access classified information with other NISP requirements and procedures. On the other side of the equation, this NISP regulation gives policy direction and establishes responsibilities for the agencies that release classified information *to* private sector entities to ensure that the agencies provide consistent oversight of entity programs. We are therefore proposing revisions to the regulation to add the insider threat requirements that pertain to NISP oversight by agencies; similar provisions have been added to the NISPOM for private sector entities to follow. The NISP CSAs, ISOO, and the National Insider Threat Task Force (NITTF) collaborated on the proposed insider threat provisions that are incorporated.

During review of the regulation, the working group determined that, although the NISPOM provides requirements and procedures for entities, this regulation did not include many of the coinciding oversight requirements for agencies. We therefore expanded the revision to include adding aspects of NISP implementation for which the agencies have a responsibility that weren't already spelled out in the regulation. These proposed changes include adding responsibility provisions for CSAs and Government contracting activities (GCAs), standards by which they make entity and employee eligibility determinations for access to classified information,

standards for assessing foreign ownership, control, or influence and for mitigating or negating it, and identifying CSA and non-CSA agency responsibilities for security classification and for authorizing entity information systems to process classified information. While CSAs and other agencies have been carrying out these responsibilities since the establishment of the NISP under E.O. 12829, and they have been spelled out in the NISPOM, they were not previously included in this regulation. We are including them to ensure agencies consistently apply the NISP requirements for all entities that have access to classified information and thereby aid in reducing processing burdens on entities. This affords agencies the opportunity to ensure that they are complying with existing NISP requirements, to include verifying that all current contracts or agreements with contractors, licensees, or grantees include appropriate security requirements. E.O. 12829 was amended by E.O. 13691, Promoting Private Sector Cybersecurity Information Sharing, in February 2015. The amendment established the DHS as a CSA, not limited to the classified critical infrastructure protection program (CCIPP). As part of its CSA responsibilities, DHS will perform oversight of critical sector entities participating in the CCIPP. We also incorporated DHS responsibilities as a CSA and the provisions of the CCIPP into this revision. We have also made some proposed revisions to more clearly set out items that were already in the regulation. One such proposed change is the approach to reciprocity. Because of the separate and unique authorities of the CSAs, one CSA might not, in some cases, reciprocally accept entity eligibility determinations made by another CSA. However, the proposed revision stipulates that CSAs will not require entities to go through duplicate steps for eligibility determinations. This should help reduce and streamline eligibility determinations for entities receiving classified information from more than one agency.

We are also proposing some new, more general terminology (like "entity eligibility determination," which describes a process all CSAs do, instead of "facility security clearance (FCL)," which is an agency-specific term for a favorable determination resulting from that process). Our goal is to create a common framework that all CSAs can effectively use because it sets out requirements in terms that encompass CSA processes for varying types of classified information under the NISP. These terminology changes do not preclude the CSAs from using their traditional terminology in agency policies that implement this rule or in the NISPOM.

The NISPOM currently includes a limited facility security clearance as an option for agencies to consider when foreign ownership, control, or influence (FOCI) of an entity cannot be mitigated or negated. We have added the limited eligibility determination option to this regulation, but have also expanded it to include limited eligibility for entities that are not under FOCI, but for which an agency considers it appropriate to limit access to a specific and narrow purpose.

In addition, we have made some drafting changes to make the regulation more readable.

Regulatory analysis

The Office of Management and Budget (OMB) has reviewed this proposed regulation.

Review under Executive Orders 12866 and 13563

Executive Order 12866, Regulatory Planning and Review, 58 FR 51735 (September 30, 1993), and Executive Order 13563, Improving Regulation and Regulation Review, 76 FR 23821 (January 18, 2011), 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, distributive impacts, and equity). This proposed rule is "significant" under

Executive Order 12866, sec. 3(f), but is not a major rule as defined in 5 U.S.C. Chapter 8, Congressional Review of Agency Rulemaking. The Office of Management and Budget (OMB) has reviewed this proposed regulation.

Review under the Regulatory Flexibility Act (5 U.S.C. 601, *et seq.*)

This review requires an agency to prepare an initial regulatory flexibility analysis and publish it when the agency publishes the proposed rule. This requirement does not apply if the agency certifies that the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities (5 U.S.C. 603). As required by the Regulatory Flexibility Act, we certify that this proposed rulemaking will not have a significant impact on a substantial number of small entities because it applies only to Federal agencies. This regulation does not establish requirements for entities; those requirements are established in the NISPOM. This rule sets out coinciding requirements for agencies. However, agencies implementing this regulation will do so through contracts with businesses (as well as other agreements with entities) and thus it indirectly affects those entities. Agencies have been applying the requirements and procedures contained in the NISPOM (and, to a lesser extent, contained in this regulation) to entities for 20 years, with the exception of insider threat provisions added to the NISPOM in 2016, and the proposed additions to this regulation do not substantially alter those requirements. Most of the provisions being added to this regulation have applied to entities through the NISPOM; we are simply incorporating the agency responsibilities for those requirements into the regulation. Other revisions to this regulation are primarily administrative, except the new insider threat requirements. The insider threat requirements make minor additions to training, oversight, information system security, and similar functions already being conducted by entities, and thus will not have a significant economic impact on a substantial number of small business entities.

Review under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*)

This proposed rule contains information collection activities that are subject to review and approval by the Office of Management and Budget (OMB) under the Paperwork Reduction Act. We refer to the following OMB-approved DoD information collection in §§ 2004.34(b), 2004.34(c)(1) of this regulation: OMB control No. 0704-0194, SF 328, Certificate Pertaining to Foreign Interests, approved through September 30, 2019. DoD published the information collection notice in the *Federal Register* in May 2015 (80 FR 27938, May 15, 2015) for public comment, and the notice of OMB review in the *Federal Register* in July 2016 (81 FR 47790, July 22, 2016), providing a second opportunity for public comment.

Review under Executive Order 13132, Federalism, 64 FR 43255 (August 4, 1999)

Review under Executive Order 13132 requires that agencies review regulations for federalism effects on the institutional interest of states and local governments, and, if the effects are sufficiently substantial, prepare a Federal assessment to assist senior policy makers. This proposed rule will not have any direct effects on State and local governments within the meaning of the Executive Order. Therefore, this rule does not include a federalism assessment.

List of Subjects in 32 CFR Part 2004

Classified information, National Industrial Security Program.

For the reasons stated in the preamble, the National Archives and Records Administration proposes to revise 32 CFR part 2004 to read as follows:

PART 2004—NATIONAL INDUSTRIAL SECURITY PROGRAM (NISP)

Subpart A—Implementation and Oversight

2004.1 Purpose and scope.

Authority: Section 102(b)(1) of E.O. 12829 (January 6, 1993), as amended by E.O. 12885 (December 14, 1993), E.O. 13691 (February 12, 2015), and section 4 of E.O. 13708 (September 30, 2015).

Subpart A—Implementation and Oversight

§ 2004.1 Purpose and scope.

(a) This part sets out the National Industrial Security Program (”NISP” or ”the Program”) governing the protection of executive-branch agency classified information released to Federal contractors, licensees, grantees, and certificate holders. It establishes uniform standards throughout the Program, and helps agencies implement requirements in E.O. 12829, National Industrial Security Program, as amended by E.O. 12558 and E.O.13691 (collectively referred to

as ”E.O. 12829”), E.O. 13691, Promoting Private Sector Cybersecurity Information Sharing, and E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information. It applies to any executive branch agency that releases classified information to current, prospective, or former Federal contractors, licensees, grantees, or certificate holders. However, this part does not stand alone; users should refer concurrently to the underlying executive orders for guidance. ISOO maintains policy oversight over the NISP as established by E.O.12829.

(b) This part also does not apply to release of classified information pursuant to criminal proceedings. The Classified Information Procedures Act (CIPA) (18 U.S.C. Appendix 3) governs release of classified information in criminal proceedings.

(c) Nothing in this part supersedes the authority of the Secretary of Energy or the Nuclear Regulatory Commission under the Atomic Energy Act of 1954, as amended (42 U.S.C. 2011, *et seq.*) (collectively referred to as “the Atomic Energy Act”); the authority of the Director of National Intelligence (or any intelligence community element) under the Intelligence Reform and Terrorism Prevention Act of 2004 (Pub.L. 108-458), the National Security Act of 1947 as amended (50 U.S.C. 401, *et seq.*), and E.O. 12333 (December 4, 1981), as amended by E.O. 13355, Strengthened Management of the Intelligence Community (August 27, 2004) and E.O. 13470, Further Amendments to Executive Order 12333 (July 30, 2008) (collectively referred to as “E.O. 12333”); or the authority of the Secretary of Homeland Security, as the Executive Agent for the Classified National Security Information Program established under E.O. 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities (August 18, 2010), or as established by E. O. 13284, Amendment of Executive Orders,

and Other Actions, in Connection with the Establishment of the Department of Homeland Security (January 23, 2003).

§ 2004.4 Definitions that apply to this part.

(a) *Access* is the ability or opportunity to gain knowledge of classified information.

(b) *Agency(ies)* are 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 part.

(c) *Classified Critical Infrastructure Protection Program (CCIPP)* is the DHS program established by E.O. 13691, "Promoting Private Sector Cybersecurity Information Sharing." The Government uses this program to share classified threat information with employees of private sector entities that own or operate critical infrastructure. Critical infrastructure refers to systems and assets, whether physical or virtual, so vital to the United States that incapacitating or destroying such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. These entities include banks and power plants, among others. The sectors of critical infrastructure are listed in Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* (February 12, 2013).

(d) *Classified Critical Infrastructure Protection Program (CCIPP) security point of*

contact (security POC) is an official whom a CCIPP entity designates to maintain eligibility information about the entity and its cleared employees, and to report that information to DHS. The CCIPP security POC must be eligible for access to classified information.

(e) *Classified information* is information the Government designates as requiring protection against unauthorized disclosure in the interest of national security, pursuant to E.O. 13526, Classified National Security Information, or any predecessor order, and the Atomic Energy Act of 1954, as amended. Classified information includes national security information (NSI), restricted data (RD), and formerly restricted data (FRD), regardless of its physical form or characteristics (including tangible items other than documents).

(f) *Cognizance* is the area over which a CSA has operational oversight. Normally, a statute or executive order establishes a CSA's cognizance over certain types of information, programs, or non-CSA agencies, although CSAs may also have cognizance through an agreement with another CSA or non-CSA agency or an entity. A CSA may have cognizance over a particular type(s) of classified information based on specific authorities (such as those listed in 2004.1(d)), and a CSA may have cognizance over certain agencies or cross-agency programs (such as DoD's cognizance over non-CSA agencies as the EA for NISP, or ODNI's oversight (if applicable) of all intelligence community elements within the executive branch). Entities fall under a CSA's cognizance when they enter or compete to enter contracts or agreements to access classified information under the CSA's cognizance, including when they enter or compete to enter such contracts or agreements with a non-CSA agency or another entity under the CSA's cognizance.

(g) *Cognizant security agencies (CSAs)* are the agencies E.O. 12829, sec. 202, designates as having NISP implementation and security responsibilities for their own agencies (including component agencies) and any entities and non-CSA agencies under their cognizance. The CSAs

are: Department of Defense (DoD); Department of Energy (DOE); Nuclear Regulatory Commission (NRC); Office of the Director of National Intelligence (ODNI); and Department of Homeland Security (DHS).

(h) *Cognizant security office (CSO)* is an organizational unit to which the head of a CSA delegates authority to administer industrial security services on behalf of the CSA.

(i) *Contracts or agreements* are any type of arrangement between an agency and an entity or an agency and another agency. They include, but are not limited to, contracts, sub-contracts, licenses, certificates, memoranda of understanding, inter-agency service agreements, other types of documents or arrangements setting out responsibilities, requirements, or terms agreed upon by the parties, programs, projects, and other legitimate U.S. or foreign government requirements. FOCI mitigation or negation measures, such as Voting Trust Agreements, that have the word "agreement" in their title are not included in the term "agreements" within this part.

(j) *Controlling agency* is an agency that owns or controls certain types of proscribed information and thus has authority over access to or release of the proscribed information. For communications security information (COMSEC), the controlling agency is NSA; for restricted data (RD), the controlling agency is DOE; and for sensitive compartmented information (SCI), the controlling agency is ODNI. For Top Secret and SAP information, the controlling agency is always the same agency as the GCA.

(k) *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), a specific location or facility, or the headquarters/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 part 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.

(l) *Entity eligibility determination* is 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). Eligibility determinations may be broad or limited to specific contracts, sponsoring agencies, or circumstances. A favorable 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. Some CSAs refer to their favorable determinations as facility security clearances (FCL). A favorable entity eligibility determination does not convey authority to store classified information.

(m) *Foreign interest* is 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 United States citizen or national.

(n) *Government contracting activity (GCA)* is an agency component or subcomponent to

which the agency head delegates broad authority regarding acquisition functions. A foreign government may also be a GCA.

(o) *Industrial security services* are those activities performed by a CSA to verify that an entity is protecting classified information. They include, but are not limited to, conducting oversight reviews, making eligibility determinations, and providing agency and entity guidance and training.

(p) *Insider(s)* are entity employees who are eligible to access classified information and may be authorized access to any U.S. Government or entity resource (such as personnel, facilities, information, equipment, networks, or systems).

(q) *Insider threat* is 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 entity or program information to the extent that the information impacts the entity's or agency's obligations to protect classified information.

(r) *Insider threat response action(s)* are actions (such as investigations) an agency takes to ascertain whether an insider threat exists, and actions the agency takes to mitigate the threat. Agencies may conduct insider threat response actions through their counterintelligence (CI), security, law enforcement, or inspector general organizations, depending on the statutory authority and internal policies that govern the agency.

(s) *Insider threat program senior official (SO)* is the official an agency head or entity designates with responsibility to manage, account for, and oversee the agency's or entity's insider threat program, pursuant to the National Insider Threat Policy and Minimum Standards. An agency may have more than one insider threat program SO.

(t) *Key managers and officials (KMO)* are the senior management official (or authorized

executive official under CCIPP), the entity's security officer (or security POC under CCIPP), the insider threat program senior official, and other entity employees whom the responsible CSA identifies as having authority, direct or indirect, to influence or decide matters affecting the entity's management or operations, its classified contracts, or national security interests. They may include individuals who hold majority ownership interest in the entity (in the form of stock or other ownership interests).

(u) *Proscribed information* is information that is classified as top secret (TS) information; communications security (COMSEC) information (excluding controlled cryptographic items when un-keyed or utilized with unclassified keys); restricted data (RD); special access program information (SAP); or sensitive compartmented information (SCI).

(v) *Security officer* is a U.S. citizen employee the entity designates to supervise and direct security measures implementing NISPOM (or equivalent; such as DOE Orders) requirements. Some CSAs refer to this position as a facility security officer (FSO). The security officer must complete security training specified by the responsible CSA, and must have and maintain an employee eligibility determination level that is at least the same level as the entity's eligibility determination level.

(w) *Senior agency official for NISP (SAO for NISP)* is the official an agency head designates to direct and administer the agency's National Industrial Security Program.

(x) *Senior management official (SMO)* is the person in charge of an entity. Under the CCIPP, this is the authorized executive official with authority to sign the security agreement with DHS.

(y) *Sub-entity* is an entity's branch or division, another type of sub-element, a sub-contractor, subsidiary, or other subordinate or connected entity. Sub-entities fall under the definition of

"entity," but this part refers to them as sub-entities when necessary to distinguish such entities from prime contractor or parent entities. See definition of "entity" at § 2004.4(k) for more context.

§ 2004.10 Responsibilities of the Director, Information Security Oversight Office (ISOO).

The Director, ISOO:

(a) Implements E.O. 12829, including ensuring that:

(1) The NISP operates as a single, integrated program across the executive branch of the Federal Government (i.e., such that agencies that release classified information to entities adhere to NISP principles);

(2) A responsible CSA oversees each entity's NISP implementation in accordance with § 2004.22;

(3) All agencies that contract for classified work include the Security Requirements clause, 48 CFR 52.204–2, from the Federal Acquisition Regulation (FAR), or an equivalent clause, in contracts that require access to classified information;

(4) Those agencies for which the Department of Defense (DoD) serves as the CSA or provides industrial security services have agreements with DoD defining the Secretary of Defense's responsibilities on behalf of their agency;

(5) Each CSA issues directions to entities under their cognizance that are consistent with the NISPOM insider threat guidance;

(6) CSAs share with each other, as lawful and appropriate, relevant information about entity employees that indicates an insider threat; and

(7) CSAs conduct ongoing analysis and adjudication of adverse or relevant information about entity employees that indicates an insider threat.

(b) Raises an issue to the National Security Council (NSC) for resolution if the EA's NISPOM coordination process cannot reach a consensus on NISPOM security standards (see §2004.20(d)).

§ 2004.11 CSA and agency implementing regulations, internal rules, or guidelines.

(a) Each CSA implements NISP practices in part through policies and guidelines that are consistent with this part, so that agencies for which it serves as the CSA are aware of appropriate security standards, engage in consistent practices with entities, and so that practices effectively protect classified information those entities receive (including foreign government information that the U.S. Government must protect in the interest of national security).

(b) Each CSA must also routinely review and update its NISP policies and guidelines and promptly issue revisions when needed (including when a change in national policy necessitates a change in agency NISP policies and guidelines).

(c) Non-CSA agencies may choose to augment CSA NISP policies or guidelines as long as the agency policies or guidelines are consistent with the CSA's policies or guidelines and this part.

§ 2004.12 ISOO review of agency NISP implementation.

(a) ISOO fulfills its oversight role based, in part, on information received from NISP Policy Advisory Committee (NISPPAC) members, from on-site reviews that ISOO conducts under the

authority of E.O. 12829, and from any submitted complaints and suggestions. ISOO reports findings to the responsible CSA or agency.

(b) ISOO reviews agency policies and guidelines to ensure consistency with NISP policies and procedures. ISOO may conduct reviews during routine oversight visits, when a problem or potential problem comes to ISOO's attention, or after a change in national policy that impacts agency policies and guidelines. ISOO provides the responsible agency with findings from these reviews.

Subpart B — Administration

§ 2004.20 National Industrial Security Program Executive Agent and Operating Manual (NISPOM).

(a) The executive agent (EA) for NISP is the Secretary of Defense. The EA:

(1) Provides industrial security services for agencies that are not CSAs but that release classified information to entities. The EA provides industrial security services only through an agreement with the agency. Non-CSA agencies must enter an agreement with the EA and comply with EA industrial security service processes before releasing classified information to an entity;

(2) Provides services for other CSAs by agreement; and

(3) Issues and maintains the National Industrial Security Program Operating Manual (NISPOM) in consultation with all affected agencies and with the concurrence of the other CSAs.

(b) The NISPOM sets out the procedures and standards that entities must follow during all

phases of the contracting process to safeguard any classified information an agency releases to an entity. The NISPOM requirements may apply to the entity directly (i.e., through FAR clauses or other contract clauses referring entities to the NISPOM) or through equivalent contract clauses or requirements documents that are consistent with NISPOM requirements.

(c) The EA, in consultation with all affected agencies and with the concurrence of the other CSAs, develops the requirements, restrictions, and safeguards contained in the NISPOM. The EA uses security standards applicable to agencies as the basis for developing NISPOM entity standards to the extent practicable and reasonable.

(d) The EA also facilitates the NISPOM coordination process, which addresses issues raised by entities, agencies, ISOO, or the NISPPAC, including requests to create or change NISPOM security standards.

§ 2004.22 Agency responsibilities.

(a) *Agency categories and general areas of responsibility*. (1) Federal agencies fall into two categories for the purpose of NISP responsibilities:

(i) CSAs. CSAs are responsible for carrying out NISP implementation within their agency, for providing NISP industrial security services on behalf of non-CSA agencies by agreement when authorized, and for overseeing NISP compliance by entities that access classified information under the CSA's cognizance. When the CSA has oversight responsibilities for a particular non-CSA agency or for an entity, the CSA also functions as the responsible CSA;

(ii) Non-CSA agencies. Non-CSA agencies are responsible for entering agreements with a designated CSA for industrial security services, and are responsible for carrying out NISP

implementation within their agency consistently with the agreement, the CSA's guidelines and procedures, and this part;

(2) Agencies that are components of another agency. Component agencies do not have itemized responsibilities under this part and do not independently need to enter agreements with a CSA, but they follow, and may have responsibilities under, implementing guidelines and procedures established by their CSA or non-CSA agency, or both.

(b) *Responsible CSA role*. (1) The responsible CSA is the CSA (or its delegated CSO) that provides NISP industrial security services on behalf of an agency, determines an entity's eligibility for access, and monitors and inspects an entity's NISP implementation.

(2) In general, the goal is to have one responsible CSA for each agency and for each entity, to minimize the burdens that can result from complying with differing CSA procedures and requirements.

(i) With regard to agencies, NISP accomplishes this goal by a combination of designated CSAs and agreements between agencies and CSAs.

(ii) With regard to entities, CSAs strive to reduce the number of responsible CSAs for a given entity as much as possible. To this end, when more than one CSA releases classified information to a given entity, those CSAs agree on which is the responsible CSA. However, due to certain unique agency authorities, there may be circumstances in which a given entity is under the oversight of more than one responsible CSA.

(3) *Responsible CSA for agencies*. (i) In general, each CSA serves as the responsible CSA for classified information that it (or any of its component agencies) releases to entities, unless it enters an agreement otherwise with another CSA.

(ii) DoD serves as the responsible CSA for DHS with the exception of the CCIPP, based on an agreement between the two CSAs.

(iii) DoD serves as the responsible CSA on behalf of all non-CSA agencies, except CSA components, based on E.O. 12829 and its role as NISP EA.

(iv) ODNI serves as the responsible CSA for CIA.

(4) *Responsible CSA for entities*. When determining the responsible CSA for a given entity, the involved CSAs consider, at a minimum: retained authorities, the information's classification level, number of classified contracts, location, number of Government customers, volume of classified activity, safeguarding requirements, responsibility for entity employee eligibility determinations, and any special requirements.

(5) Responsible CSAs may delegate oversight responsibility to a cognizant security office (CSO) through CSA policy or by written delegation. The CSA must inform entities under its cognizance if it delegates responsibilities. For purposes of this rule, the term CSA also refers to the CSO.

(c) *CSA responsibilities*. (1) The CSA may perform GCA responsibilities as its own GCA.

(2) As CSA, the CSA performs or delegates the following responsibilities:

(i) Designates a CSA senior agency official (SAO) for NISP;

(ii) Identifies the insider threat senior official (SO) to the Director, ISOO;

(iii) Shares insider threat information with other CSAs, as lawful and appropriate, including information that indicates an insider threat about entity employees eligible to access classified information;

(iv) Acts upon and shares -- with security management, GCAs, insider threat program employees, and Government program and CI officials -- any relevant entity-reported information about security or CI concerns, as appropriate;

(v) Submits reports to ISOO as required by this part; and

(vi) Develops, coordinates, and provides concurrence on changes to the NISPOM when requested by the EA.

(3) As a responsible CSA, the CSA also performs or delegates the following responsibilities:

(i) Determines whether an entity is eligible for access to classified information (see § 2004.32);

(ii) Allocates funds, ensures appropriate investigations are conducted, and determines entity employee eligibility for access to classified information (see § 2004.36);

(iii) Reviews and approves entity safeguarding measures, including making safeguarding capability determinations (see § 2004.38);

(iv) Conducts periodic security reviews of entity operations (see § 2004.26) to determine that entities: effectively protect classified information provided to them; and follow NISPOM (or equivalent) requirements;

(v) Provides and regularly updates guidance, training, training materials, and briefings to entities on:

(A) Entity implementation of NISPOM (or equivalent) requirements, including: responsibility for protecting classified information, requesting NISPOM interpretations, establishing training programs, and submitting required reports;

(B) Initial security briefings and other briefings required for special categories of information;

(C) Authorization measures for information systems processing classified information (except DHS) (see § 2004.40);

(D) Security training for security officers (or CCIPP POCs) and other employees whose official duties include performing NISP-related functions;

(E) Insider threat programs in accordance with the National Insider Threat Policy and Minimum Standards; and

(F) Other guidance and training as appropriate;

(vi) Establishes a mechanism for entities to submit requests for waivers to NISPOM (or equivalent) provisions;

(vii) Reviews, continuously analyzes, and adjudicates, as appropriate, reports from entities regarding events that:

(A) Impact the status of the entity's eligibility for access to classisfied information;

(B) Impact an employee's eligibility for access;

(C) May indicate an employee poses an insider threat;

(D) Affect proper safeguarding of classified information; or

(E) Indicate that classified information has been lost or compromised.

(viii) Verifies that reports offered in confidence and so marked by an entity may be withheld from public disclosure under applicable exemptions of the Freedom of Information Act (5 U.S.C. 552).

(ix) Requests any additional information needed from an entity about involved employees to determine continued eligibility for access to classified information when the entity reports loss, possible compromise, or unauthorized disclosure of classified information; and

(x) Posts hotline information on its website for entity access, or otherwise disseminates contact numbers to the entities for which the CSA is responsible.

(d) *Non-CSA agency head responsibilities*. The head of a non-CSA agency that is not a CSA component and that releases classified information to entities, performs the following responsibilities:

(1) Designates an SAO for the NISP;

(2) Identifies the SO for insider threat to ISOO to facilitate information sharing;

(3) Enters into an agreement with the EA (except agencies that are components of another agency or a cross-agency oversight office) to act as the responsible CSA on the agency's behalf (see paragraph (a)(1)(ii) of this section);

(4) Performs, or delegates in writing to a GCA, the following responsibilities:

(i) Provides appropriate education and training to agency personnel who implement the NISP;

(ii) Includes FAR security requirements clause 52.204–2, or equivalent (such as the DEAR clause 952.204-2), and a contract security classification specification into contracts and solicitations that require access to classified information (see § 2004.30); and

(iii) Reports to the appropriate CSA adverse information and insider threat activity pertaining to entity employees having access to classified information.

§ 2004.24 Insider threat program.

(a) Responsible CSAs oversee and analyze entity activity to ensure entities implement an insider threat program in accordance with the National Insider Threat Policy and Minimum

Standards (via requirements in the NISPOM or its equivalent) and guidance from the CSA, to include:

(1) Verifying that entities appoint SOs for insider threat;

(2) Requiring entities to monitor, report, and review insider threat program activities and response actions in accordance with the provisions set forth in the NISPOM (or equivalent);

(3) Providing entities with access to data relevant to insider threat program activities and applicable reporting requirements and procedures;

(4) Providing entities with a designated means to report insider threat-related activity; and

(5) Advising entities on appropriate insider threat training for authorized entity employees.

(b) CSAs share with other CSAs any insider threat information reported to them by entities, as lawful and appropriate.

§ 2004.26 Reviews of entity NISP implementation.

(a) The responsible CSA conducts recurring oversight reviews of entities' NISP security programs to verify that the entity is protecting classified information and is implementing the provisions of the NISPOM (or equivalent). The CSA determines the scope and frequency of reviews. The CSA generally notifies entities when a review will take place, but may also conduct unannounced reviews at its discretion.

(b) CSAs make every effort to avoid unnecessarily intruding into entity employee personal effects during the reviews.

(c) A CSA may, on entity premises, physically examine the interior spaces of containers not authorized to store classified information in the presence of the entity's representative.

(d) As part of a security review, the CSA:

(1) Verifies that the entity limits entity employees with access to classified information to the minimum number necessary to perform on classified contracts.

(2) Validates that the entity has not provided its employees unauthorized access to classified information;

(3) Reviews the entity's self-inspection program and evaluates and records the entity's remedial actions; and

(4) Verifies that the GCA approved any public release of information pertaining to a classified contract.

(e) As a result of findings during the security review, the CSA may, as appropriate, notify:

(1) GCAs if there are unfavorable results from the review; and

(2) A prime entity if the CSA discovers unsatisfactory security conditions pertaining to a sub-entity.

(f) The CSA maintains a record of reviews it conducts and the results. Based on review results, the responsible CSA determines whether an entity's eligibility for access to classified information may continue. See § 2004.32(g).

§ 2004.28 Cost reports.

(a) Agencies must annually report to the Director, ISOO, on their NISP implementation costs for the previous year.

(b) CSAs must annually collect information on NISP implementation costs incurred by entities under their cognizance and submit a report to the Director, ISOO.

Subpart C -- Operations

§ 2004.30 Security classification requirements and guidance.

(a) *Contract or agreement and solicition requirements*. (1) The GCA must incorporate FAR clause 52.204-2, Security Requirements (or equivalent set of security requirements), into contracts or agreements and solicitations requiring access to classified information.

(2) The GCA must also include a contract security classification specification (or equivalent guidance) with each contract or agreement and solicitation that requires access to classified information. The contract security classification specification (or equivalent guidance) must identify the specific elements of classified information involved in each phase of the contract or agreement life-cycle, such as:

(i) Level of classification;

(ii) Where the entity will access or store the classified information, and any requirements or limitations on transmitting classified information outside the entity;

(iii) Any special accesses;

(iv) Any classification guides or other guidance the entity needs to perform during that phase of the contract or agreement;

(v) Any authorization to disclose information about the classified contract or agreement; and

(vi) GCA personnel responsible for interpreting and applying the contract security specifications (or equivalent guidance).

(3) The GCA revises the contract security classification specification (or equivalent guidance) throughout the contract or agreement life-cycle as security requirements change.

(b) *Guidance*. Classification guidance is the exclusive responsibility of the GCA. The GCA

prepares classification guidance in accordance with 32 CFR 2001.15, and provides appropriate security classification and declassification guidance to entities.

(c) *Requests for clarification and classification challenges*. (1)The GCA responds to entity requests for clarification and classification challenges.

(2) The responsible CSA assists entities to obtain appropriate classification guidance from the GCA, and to obtain a classification challenge response from the GCA.

(d) *Instructions upon contract or agreement termination*. (1) The GCA provides instructions to the entity for returning or disposing of classified information upon contract or agreement termination or when an entity no longer has a legitimate need to retain or possess classified information.

(2) The GCA also determines whether the entity may retain classified information for particular purposes after the contract or agreement terminates, and if so, provides written authorization to the entity along with any instructions or limitations (such as which information, for how long, etc).

§ 2004.32 Determining entity eligibility for access to classified information.

(a) *Eligibility determinations*. (1) The responsible CSA determines whether an entity is eligible for access to classified information. An entity may not have access to classified information until the responsible CSA determines that it meets all the requirements in this section. In general, the entity must be eligible to access classified information at the appropriate level before the CSA may consider any of the entity's subsidiaries, sub-contractors, or other sub-entities for eligibility. However, when the subsidiary will perform all classified work, the CSA may instead exclude the parent entity from access to classified information rather than

determining its eligibility. In either case, the CSA must consider all information relevant to assessing whether the entity's access poses an unacceptable risk to national security interests.

(2) A favorable access eligibility determination is not the same as a safeguarding capability determination. Entities may access classified information with a favorable eligibility determination, but may possess classified information only if the CSA determines both access eligibility and safeguarding capability, based on the GCA's requirement in the contract security classification specification (or equivalent).

(3) If an entity has an existing eligibility determination, a CSA will not duplicate eligibility determination processes performed by another CSA. If a CSA cannot acknowledge an entity eligibility determination to another CSA, that entity may be subject to duplicate processing.

(4) Each CSA maintains a record of its entities' eligibility determinations (or critical infrastructure entity eligibility status under the CCIPP, for DHS) and responds to inquiries from GCAs or entities, as appropriate and to the extent authorized by law, regarding the eligibility status of entities under their cognizance.

(b) *Process*. (1) The responsible CSA provides guidance to entities on the eligibility determination process and on how to maintain eligibility throughout the period of the agreement or as long as an entity continues to need access to classified information in connection with a legitimate U.S. or foreign government requirement.

(2) The CSA coordinates with appropriate authorities to determine whether an entity meets the eligibility criteria in paragraph (e) of this section. This includes coordinating with appropriate U.S. Government regulatory authorities to determine entity compliance with laws and regulations.

(3) An entity cannot apply for its own eligibility determination. A GCA or an eligible entity must sponsor the entity to the responsible CSA for an eligibility determination. The GCA or eligible entity may sponsor an entity 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). An entity with limited eligibility granted under paragraph (f) of this section may sponsor a sub-entity for a limited eligibility determination for the same contract, agreement, or circumstance so long as the sponsoring entity is not under FOCI (see § 2004.34(i)).

(4) The GCA must include enough lead time in each phase of the acquisition or agreement cycle to accomplish all required security actions. Required security actions include any eligibility determination necessary for an entity to participate in that phase of the cycle. The GCA may award a contract or agreement before the CSA completes the entity eligibility determination. However, in such cases, the entity may not begin performance on portions of the contract or agreement that require access to classified information until the CSA makes a favorable entity eligibility determination.

(5) When a CSA is unable to make an eligibility determination in sufficient time to qualify an entity to participate in the particular procurement action or phase that gave rise to the GCA request (this includes both solicitation and performance phases), the GCA may request that the CSA continue the determination process to qualify the entity for future classified work, provided that the processing delay was not due to the entity's lack of cooperation.

(c) *Coverage*. (1) A favorable eligibility determination allows an entity to access classified information at the determined eligibility level, or lower.

(2) The CSA must ensure that all entities needing access to classified information as part of a legitimate U.S. or foreign government requirement have or receive a favorable eligibility determination before accessing classified information. This includes both prime or parent entities and sub-entities, even in cases in which an entity intends to have the classified work performed only by sub-entities. A prime or parent entity must have a favorable eligibility determination at the same classification level or higher than its sub-entity(ies), unless the CSA determined that the parent entity could be effectively excluded from access (see paragraph (a)(1) of this section).

(3) If a parent and sub-entity need to share classified information with each other, the CSA must validate that both the parent and the sub-entity have favorable eligibility determinations at the level required for the classified information prior to sharing the information.

(d) *DHS Classified Critical Infrastructure Protection Program (CCIPP)*. DHS shares classified cybersecurity information with certain employees of entities under the Classified Critical Infrastructure Protection Program (CCIPP). The CCIPP applies only to entities that do not need to store classified information, have no other contracts or agreements already requiring access to classified information, and are not already determined eligible for access to classified information. DHS establishes and implements procedures consistent with the NISP to determine CCIPP entity eligibility for access to classified information.

(e) *Eligibility criteria*. An entity must meet the following requirements to be eligible to access classified information:

(1) It must need to access classified information as part of a legitimate U.S. Government or foreign government requirement, and access must be consistent with U.S. national security interests as determined by the CSA;

(2) It must be organized and existing under the laws of any of the 50 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 an American Indian or Alaska native tribe formally acknowledged by the Assistant Secretary – Indian Affairs, of the U.S. Department of the Interior;

(3) It must be located in the United States or its territorial areas;

(4) It must have a record of compliance with pertinent laws, regulations, and contracts (or other relevant agreements).

(5) Its KMOs must each have and maintain eligibility for access to classified information that is at least the same level as the entity eligibility level;

(6) It and all of its KMOs must not be excluded by a Federal agency, contract review board, or other authorized official from participating in Federal contracts or agreements;

(7) It must meet all requirements the CSA or the authorizing law, regulation, or Government-wide policy establishes for access to the type of classified information or program involved; and

(8) If the CSA determines the entity is under foreign ownership, control, or influence (FOCI), the responsible CSA must:

(i) Agree that sufficient security measures are in place to mitigate or negate risk to national security interests due to the FOCI (see § 2004.34);

(ii) Determine that it is appropriate to grant eligibility for a single, narrowly defined purpose (see § 2004.34(i)); or

(iii) Determine that the entity is not eligible to access classified information.

(9) DoD and DOE cannot award a contract involving access to proscribed information to an entity effectively owned or controlled by a foreign government unless the Secretary of the

agency first issues a waiver (see 10 U.S.C. 2536). A waiver is not required if the CSA determines the entity is eligible and it agrees to establish a voting trust agreement (VTA) or proxy agreement (PA) (see § 2004.34(f)) because both VTAs and PAs effectively negate foreign government control.

(f) *Limited entity eligibility determination*. CSAs may choose to allow GCAs to request limited entity eligibility determinations (this is not the same as limited entity eligibility in situations involving FOCI when the FOCI is not mitigated or negated; for more information on limited entity eligibility in such FOCI cases, see § 2004.34(i)). If a CSA permits GCAs to request a limited entity eligibility determination, it must set out parameters within its implementing policies that are consistent with the requirements below:

(1) The GCA, or an entity with limited eligibility, must first request a limited entity eligibility determination from the CSA for the relevant entity and provide justification for limiting eligibility in that case;

(2) Limited entity eligibility is specific to the requesting GCA's classified information, and to a single, narrowly defined contract, agreement, or circumstance;

(3) The entity must otherwise meet the requirements for entity eligibility set out in this part;

(4) The CSA documents the requirements of each limited entity eligibility determination it makes, including the scope of, and any limitations on, access to classified information;

(5) The CSA verifies limited entity eligibility determinations only to the requesting GCA or entity. In the case of multiple limited entity eligibility determinations for a single entity, the CSA verifies each one separately only to its requestor; and

(6) CSAs administratively terminate the limited entity eligibility when there is no longer a need for access to the classified information for which the CSA approved the limited entity eligibility.

(g) *Terminating or revoking eligibility*. (1) The responsible CSA terminates the entity's eligible status when the entity no longer has a need for access to classified information.

(2) The responsible CSA revokes the entity's eligible status if the entity is unable or unwilling to protect classified information.

(3) The CSA coordinates with the GCA(s) to take interim measures, as necessary, toward either termination or revocation.

§ 2004.34 Foreign ownership, control, or influence (FOCI).

(a) *FOCI determination*. A U.S. entity is under foreign ownership, control, or influence (FOCI) when:

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

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

(ii) Adversely affect performance of a classified contract or agreement; and

(2) The foreign interest exercises that power:

(i) Directly or indirectly;

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

(iii) By the ability to control or influence the election or appointment of one or more members to the entity's governing board (e.g. board of directors, board of managers, board of trustees) or its equivalent; or

(iv) Prospectively (i.e., is not currently exercising the power, but could).

(b) *CSA guidance*. The CSA establishes guidance for entities on filling out and submitting a Standard Form (SF) 328, Certificate Pertaining to Foreign Interests (OMB Control No. 0704-0194), and on reporting changes in circumstances that might result in a determination that the entity is under FOCI or is no longer under FOCI. The CSA also advises entities on the Government appeal channels for disputing CSA FOCI determinations.

(c) *FOCI factors*. To determine whether an entity is under FOCI, the CSA analyzes available information to determine the existence, nature, and source of FOCI. The CSA:

(1) Considers information the entity or its parent provides on the SF 328 (OMB Control No. 0704-0194), and any other relevant information; and

(2) Considers in the aggregate the following factors about the entity:

(i) Record of espionage against U.S. targets, either economic or Government;

(ii) Record of enforcement actions against the entity for transferring technology without authorization;

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

(iv) Type and sensitivity of the information the entity would access;

(v) 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;

(vi) Nature of any relevant bilateral and multilateral security and information exchange agreements;

(vii) Ownership or control, in whole or in part, by a foreign government; and

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

(d) *Entity access while under FOCI.* (1) If the CSA is determining whether an entity is eligible to access classified information and finds that the entity is under FOCI, the CSA must consider the entity ineligible for access to classified information. The CSA and the entity may then attempt to negotiate FOCI mitigation or negation measures sufficient to permit a favorable eligibility determination.

(2) The CSA may not determine that the entity is eligible to access classified information until the entity has put into place appropriate security measures to negate or mitigate FOCI or is otherwise no longer under FOCI. If the degree of FOCI is such that no mitigation or negation efforts will be sufficient, or access to classified information would be inconsistent with national security interests, then the CSA will determine the entity ineligible for access to classified information.

(3) If an entity comes under FOCI, the CSA may allow the existing eligibility status to continue while the CSA and the entity negotiate acceptable FOCI mitigation or negation measures, as long as there is no indication that classified information is at risk. If the entity does not actively negotiate mitigation or negation measures in good faith, or there are no appropriate measures that will remove the possibility of unauthorized access or adverse effect on the entity's performance of contracts or agreements involving classified information, the CSA will take steps, in coordination with the GCA, to terminate eligibility.

(e) *FOCI and entities under the CCIPP*. DHS may sponsor, as part of the CCIPP, a U.S. entity that is under FOCI, under the following circumstances:

(1) The Secretary of DHS proposes appropriate FOCI risk mitigation or negation measures (see paragraph (f) of this section) to the other CSAs and ensures the anticipated release of classified information:

(i) Is authorized for release to the country involved;

(ii) Does not include information classified under the Atomic Energy Act; and

(iii) Does not impede or interfere with the entity's ability to manage and comply with regulatory requirements imposed by other Federal agencies, such as the State Department's International Traffic in Arms Regulation.

(2) If the CSAs agree the mitigation or negation measures are sufficient, DHS may proceed to enter a CCIPP information sharing agreement with the entity. If one or more CSAs disagree, the Secretary of DHS may seek a decision from the Assistant to the President for National Security Affairs before entering a CCIPP information sharing agreement with the entity.

(f) *Mitigation or negation measures to address FOCI*. (1) The CSA-approved mitigation or negation measures must assure that the entity can offset FOCI by effectively denying unauthorized people or entities access to classified information and preventing the foreign interest from adversely impacting the entity's performance on classified contracts or agreements.

(2) Any mitigation or negation measures the CSA approves for an entity must not impede or interfere with the entity's ability to manage and comply with regulatory requirements imposed by other Federal agencies (such as Department of State's International Traffic in Arms Regulation).

(3) If the CSA approves a FOCI mitigation or negation measure for an entity, it may agree that the measure, or particular portions of it, may apply to all of the present and future sub-entities within the entity's organization.

(4) Mitigation or negation options are different for ownership versus control or influence; ownership necessitates a stronger mitigation or negation measure.

(5) Methods to mitigate foreign control or influence (unrelated to ownership) may include:

(i) Assigning specific oversight duties and responsibilities to independent board members;

(ii) Formulating special executive-level security committees to consider and oversee matters that affect entity performance on classified contracts or agreements;

(iii) Modifying or terminating loan agreements, contracts, agreements, and other understandings with foreign interests;

(iv) Diversifying or reducing foreign-source income;

(v) Demonstrating financial viability independent of foreign interests;

(vi) Eliminating or resolving problem debt;

(vii) Separating, physically or organizationally, the entity component performing on classified contracts or agreements;

(viii) Adopting special board resolutions; and

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

(6) Methods to mitigate or negate foreign ownership include:

(i) Board resolutions. The CSA and the entity may agree to a board resolution when a foreign interest does not own voting interests sufficient to elect, or is otherwise not entitled to representation on, the entity's governing board. The resolution must identify the foreign

shareholders and their representatives (if any), note the extent of foreign ownership, certify that the foreign shareholders and their representatives will not require, will not have, and can be effectively excluded from, access to all classified information, and certify that the entity will not permit the foreign shareholders and their representatives to occupy positions that might enable them to influence the entity's policies and practices, affecting its performance on classified contracts or agreements.

(ii) Security control agreements (SCAs). The CSA and the entity may agree to use an 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. At least one cleared U.S. citizen must serve as an outside director on the entity's governing board.

(iii) Special security agreements (SSAs). The CSA and the entity may agree to use an SSA when a foreign interest effectively owns or controls an entity. 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. When a GCA requires an entity to have access to proscribed information, and the CSA proposes or approves an SSA as the mitigation measure, the GCA must also make a national interest determination (NID) before the CSA can determine an entity's eligibility for access. See paragraph (h) of this section for more information on NIDs.

(iv) Voting trust agreements (VTAs) or proxy agreements (PAs). The CSA and the entity may agree to use one of these measures when a foreign interest effectively owns or controls an entity. The VTA and PA are substantially identical arrangements that vest the voting

rights of the foreign-owned stock in cleared U.S. citizens approved by the CSA. Under the VTA, the foreign owner transfers legal title in the entity to the trustees approved by the CSA. Under the PA, the foreign owner conveys their voting rights to proxy holders approved by the CSA. The entity must be organized, structured, and financed to be capable of operating as a viable business entity independently from the foreign owner. Both VTAs and PAs can effectively negate foreign ownership and control; therefore, neither imposes any restrictions on the entity's eligibility to have access to classified information or to compete for classified contracts or agreements, including those involving proscribed information. Both VTAs and PAs can also effectively negate foreign government control.

(v) Combinations of the above measures or other similar measures that effectively mitigate or negate the risks involved with foreign ownership.

(g) *Standards for FOCI mitigation or negation measures*. The CSA must include the following requirements as part of any FOCI mitigation or negation measures, to ensure that entities implement necessary security and governing controls:

(1) Annual certification and annual compliance reports by the entity's governing board and the KMOs;

(2) The U.S. Government remedies in case the entity is not adequately protecting classified information or not adhering to the provisions of the mitigation or negation measure;

(3) Supplements to FOCI mitigation or negation measures as the CSA deems necessary. In addition to the standard FOCI mitigation or negation measure's requirements, the CSA may require more procedures via a supplement, based upon the circumstances of an entity's operations. The CSA may place these requirements in supplements to the FOCI mitigation or negation measure to allow flexibility as circumstances change without having to renegotiate the

entire measure. When making use of supplements, the CSA does not consider the FOCI mitigation measure final until it approves the required supplements (e.g., technology control plan, electronic communication plan); and

(4) For agreements to mitigate or negate ownership (PAs, VTAs, SSAs, and SCAs), the following additional requirements apply:

(i) FOCI oversight. The CSA verifies that the entity establishes an oversight body consisting of trustees, proxy holders or outside directors, as applicable, and those officers or directors whom the CSA determines are eligible for access to classified information (see § 2004.36). The entity's security officer is the principal advisor to the oversight body and attends their meetings. The oversight body:

(A) Maintains policies and procedures to safeguard classified information in the entity's possession with no adverse impact on classified contract or agreement performance; and

(B) Verifies the entity is complying with the FOCI mitigation or negation measure and related documents, contract security requirements or equivalent, and the NISP;

(ii) Qualifications of trustees, proxy holders, and outside directors. The CSA determines eligibility for access to classified information for trustees, proxy holders, and outside directors at the classification level of the entity's eligibility determination. Trustees, proxy holders, and outside directors must meet the following criteria:

(A) Be resident U.S. citizens who can exercise management prerogatives relating to their position in a way that ensures that the foreign owner can be effectively insulated from the entity or effectively separated from the entity's classified work; and

(B) Be completely disinterested individuals with no prior involvement with the entity, the entities with which it is affiliated, or the foreign owner;

(C) No other circumstances that may affect an individual's ability to serve effectively; such as, the number of boards on which the individual serves, the length of time serving on any other boards.

(iii) Annual meeting. The CSA meets at least annually with the oversight body to review the purpose and effectiveness of the FOCI mitigation or negation agreement; establish a common understanding of the operating requirements and their implementation; and provide guidance on matters related to FOCI mitigation and industrial security. These meetings include a CSA review of:

(A) Compliance with the approved FOCI mitigation or negation measure;

(B) Problems regarding practical implementation of the mitigation or negation measure; and

(C) Security controls, practices, or procedures and whether they warrant adjustment; and

(iv) Annual certification. The CSA reviews the entity's annual report; addresses, and resolves issues identified in the report; and documents the results of this review and any follow-up actions.

(h) *National interest determination (NID).* (1) *Requirement for a NID.* When a GCA requires an entity to have access to proscribed information, and the CSA proposes or approves an SSA as the FOCI mitigation measure, the GCA must determine (with controlling agency concurrence when appropriate) whether releasing the proscribed information to the entity under an SSA is consistent with the national security interests of the United States. This determination is called a national interest determination (NID). A favorable NID confirms that an entity's access to the proscribed information is consistent with such interests and allows the CSA to

make a positive entity eligibility determination in such cases if the entity meets the other eligibility requirements. If the NID is not favorable, an entity may not have access to the proscribed information.

(i) The CSA requests a NID from the GCA for new contracts or agreements at any phase that requires access to proscribed information; and existing contracts or agreements (or any relevant sub-contracts or sub-agreements) when the GCA adds a requirement for access to proscribed information or adds a new sub-entity that operates under an SSA and requires access to proscribed information. The GCA may initiate a NID prior to receiving the request from the CSA, when appropriate.

(ii) While CSAs normally request NIDs on a case-by-case contract- or agreement-specific basis, the CSA, GCA, and applicable controlling agency may decide to make a NID on another basis, using criteria the CSA establishes. In such cases, the GCA provides the CSA with a written statement that the NID covers a specific contract or program and all follow-on contracts associated that program, and lists all contracts or agreements covered by the NID in cases in which the GCA can identify them.

(iii) When an entity has a favorable NID for a given contract or agreement, the CSA does not have to request a new NID for the same entity when the access requirements for proscribed information and terms remain unchanged for:

(A) Renewal of the contract or agreement;

(B) New task orders issued under the contract or agreement;

(C) A new contract or agreement that contains the same provisions as the previous (this usually applies when the contract or agreement is for a program or project); or

(D) Renewal of the SSA.

(2) *Process*. (i) The CSA requests the NID from the GCA and provides the GCA with pertinent information, such as: the FOCI assessment; a copy of the SSA; and any other relevant information that might help the GCA make its determination.

(ii) If another agency (or agencies) ~~owns or~~controls any category of the proscribed information involved, the GCA or CSA also coordinates with the controlling agency(ies) to request their concurrence on the GCA's NID. In cases involving one or more controlling agencies, a favorable NID is not final until the relevant controlling agencies concur with the determination in writing for the proscribed information under their control. The GCA or CSA provides the relevant controlling agency(ies) with: a statement that "Access to the proscribed information by the entity is consistent with the national security interests of the United States"; the FOCI assessment; a copy of the SSA; a contract security classification specification (or equivalent); justification for access and a description of the proscribed information involved; and any other relevant information that might help the controlling agency consider the request.

(iii) In cases in which the GCA has authority over all the categories of proscribed information involved, the CSA may make an entity eligibility determination or upgrade an existing eligibility level to top secret only after the GCA notifies the CSA in writing of a favorable NID, except as described in paragraph (h)(3)(iii)(A) of this section.

(iv) In cases in which the GCA requests concurrence from one or more controlling agencies, it does not notify the CSA of its NID until the controlling agency concurs. In cases in which the CSA requests concurrence from the controlling agency, the CSA may not act upon a favorable GCA NID until it also receives written concurrence from the controlling agency(ies). In both cases, the CSA may not make an eligibility determination until all the relevant

controlling agencies concur in writing on a favorable NID and the GCA notifies the CSA in writing of its final NID, except as described in paragraph (h)(3)(iii)(B) of this section.

(3) *Timing*. (i) When the GCA has authority over all of the categories of proscribed information involved, the GCA provides a final, written NID to the CSA, with a copy to the entity, within 30 days after the GCA receives the NID request .

(ii) If a controlling agency controls any of the involved categories of proscribed information, the GCA provides a final, written NID to the CSA, with a copy to the entity, within 60 days after the GCA receives the NID request.

(A) In such cases, the GCA notifies the relevant controlling agency(ies) of its NID in writing within 30 days after it receives the NID request, and each controlling agency concurs or non-concurs in writing to the GCA or CSA within the next 30 days unless there are extenuating circumstances.

(B) In cases in which there are extenuating circumstances, the controlling agency responds to the GCA or CSA within 30 days to explain the extenuating circumstances, request additional information as needed, and coordinate a plan and timeline for completion.

(iii) If the GCA cannot make the NID within the 30- or 60-day timeframes in paragraphs (h)(3)(i) and (h)(3)(ii) of this section, the GCA must notify the CSA in writing and explain the extenuating circumstances causing the delay. The GCA must provide written updates to the CSA, or its designee, every 30 days until it makes the determination. In turn, the CSA provides the entity with updates every 30 days.

(A) When the GCA has authority over all the categories of the proscribed information involved, if the GCA does not provide the CSA with a NID within 30 days, the CSA does not have to delay any longer to make the entity eligibility determination or upgrade it to top secret

and implement an SSA to wait for the NID, as long as the GCA does not indicate that the NID might be negative. However, the entity must not have access to proscribed information under a new contract until the GCA makes a favorable NID.

(B) In some cases in which one or more controlling agencies have authority over any category of the proscribed information involved, the GCA or CSA might receive concurrence on a favorable NID from some of the controlling agencies within 60 days, but not others. In such cases, the CSA may proceed with an eligibility determination or upgrade it to top secret eligibility and implement an SSA, but only for those categories of proscribed information for which a controlling agency has concurred. The entity must not have access to any category of proscribed information for which a controlling agency that has not yet concurred.

(iv) Unless cancelled sooner by the GCA that made the NID, a NID remains in effect for the duration of the contract or agreement. When a NID is not contract- or agreement-specific, the CSA, the GCA, and any applicable controlling agency determine how long the NID remains in effect based on the criteria used to make the NID.

(i) *Limited eligibility determinations (for entities under FOCI without mitigation or negation).* (1) In exceptional circumstances when an entity is under FOCI, the CSA may decide that limited eligibility for access to classified information is appropriate when the entity is unable or unwilling to implement FOCI mitigation or negation measures (this is not the same as limited eligibility in other circumstances; for more information on limited eligibility in other cases, see § 2004.32(f)).

(2) The GCA first decides whether to request a limited eligibility determination for the entity and must articulate a compelling need for it that is in accordance with U.S. national security

interests. The GCA must verify that access to classified information is essential to contract or agreement performance, and accept the risk inherent in not mitigating or negating the FOCI.

(3) The CSA may grant a limited eligibility determination if the GCA requests and the entity meets all other eligibility criteria in § 2004.32(e).

(4) A foreign government may sponsor a U.S. sub-entity of a foreign entity for limited eligibility when the foreign government desires to award a contract or agreement to the U.S. sub-entity that involves access to classified information for which the foreign government is the original classification authority (i.e., foreign government information), and there is no other need for the U.S. sub-entity to have access to classified information.

(5) Limited eligibility determinations are specific to the classified information of the requesting GCA or foreign government, and specific to a single, narrowly defined contract, agreement, or circumstance of that GCA or foreign government.

(6) The access limitations of a favorable limited eligibility determination apply to all of the entity's employees, regardless of citizenship.

(7) A limited eligibility determination is not an option for entities that require access to proscribed information when a foreign government has ownership or control over the entity. See § 2004.32(e)(9).

(8) The CSA administratively terminates the entity's limited eligibility when there is no longer a need for access to the classified information for which the CSA made the favorable limited eligibility determination. Terminating one limited eligibility status does not impact other ones the entity may have.

§ 2004.36 Determining entity employee eligibility for access to classified information.

(a) *Making employee eligibility determinations*. (1) The responsible CSA:

(i) Determines whether entity employees meet the criteria established in the Revised Adjudicative Guidelines for Determining Eligibility for Access to Classified Information issued by White House memorandum, December 29, 2005, and in accordance with applicable executive branch procedures. Entity employees must have a legitimate requirement (i.e., need to know) for access to classified information in the performance of assigned duties and eligibility must be clearly consistent with the interest of the national security.

(ii) Notifies entities of its determinations of employee eligibility for access to classified information.

(iii) Terminates eligibility status when there is no longer a need for access to classified information by entity employees.

(2) The responsible CSA maintains:

(i) SF 312s, Classified Information Nondisclosure Agreements, or other approved nondisclosure agreements, executed by entity employees, as prescribed by ODNI in accordance with 32 CFR 2001.80 and E.O. 13526; and

(ii) Records of its entity employee eligibility determinations, suspensions, and revocations.

(3) CSAs ensure that entities limit the number of employees with access to classified information to the minimum number necessary to work on classified contracts or agreements.

(4) The CSA determines the need for event-driven reinvestigations for entity employees.

(5) CSAs use the Federal Investigative Standards (FIS) issued jointly by the Suitability and Security Executive Agents.

(6) The CSA provides guidance to entities on:

(i) Requesting employee eligibility determinations, to include guidance for submitting fingerprints; and

(ii) Granting employee access to classified information when the employee has had a break in access or a break in employment.

(7) If the CSA receives adverse information about an eligible entity employee, the CSA should consider and possibly investigate to determine whether the employee's eligibility to access classified information remains clearly consistent with the interests of national security. If the CSA determines that an entity employee's continued eligibility is not in the interest of national security, the CSA implements procedures leading to suspension and ultimate revocation of the employee's eligible status, and notifies the entity.

(b) *Consultants*. A consultant is an individual under contract or agreement to provide professional or technical assistance to an entity in a capacity requiring access to classified information. A consultant is considered an entity employee for security purposes. The CSA makes eligibility determinations for entity consultants in the same way it does for entity employees.

(c) *Reciprocity.* The responsible CSA determines if an entity employee was previously investigated or determined eligible by another CSA. CSAs reciprocally accept existing employee eligibility determinations in accordance with applicable and current national level personnel security policy, and do not duplicate employee eligibility investigations conducted by another CSA.

(d) *Limited access authorization (LAA).* (1) CSAs may make LAA determinations for non-U.S. citizen entity employees in rare circumstances, when:

(i) A non-U.S. citizen employee possesses unique or unusual skill or expertise that the agency urgently needs to support a specific U.S. Government contract or agreement; and

(ii) A U.S. citizen with those skills is not available.

(2) A CSA may grant LAAs up to the secret classified level.

(3) CSAs may not use LAAs for access to:

(i) Top secret (TS) information;

(ii) RD or FRD information;

(iii) Information that a Government-designated disclosure authority has not determined releasable to the country of which the individual is a citizen;

(iv) COMSEC information;

(v) Intelligence information, to include SCI;

(vi) NATO information, except as follows: Foreign nationals of a NATO member nation may be authorized access to NATO information subject to the terms of the contract, if the responsible CSA obtains a NATO security clearance certificate from the individual's country of citizenship. NATO access is limited to performance on a specific NATO contract;

(vii) Information for which the U.S. Government has prohibited foreign disclosure in whole or in part; or

(viii) Information provided to the U.S. Government by another government that is classified or provided in confidence.

(4) The responsible CSA provides specific procedures to entities for requesting LAAs. The GCA must concur on an entity's LAA request before the CSA may grant it.

§ 2004.38 Safeguarding and marking.

(a) *Safeguarding approval*. (1) The CSA determines whether an entity's safeguarding capability meets requirements established in 32 CFR 2001, and other applicable national level policy (e.g., Atomic Energy Act for RD). If the CSA makes a favorable determination, the entity may store classified information at that level or below. If the determination is not favorable, the CSA must ensure that the entity does not possess classified information or does not possess information at a level higher than the approved safeguarding level.

(2) The CSA maintains records of its safeguarding capability determinations and, upon request from GCAs or entities, and as appropriate and to the extent authorized by law, verifies that it has made a favorable safeguarding determination for a given entity and at what level.

(b) *Marking*. The GCA provides guidance to entities that meets requirements in 32 CFR 2001.22, 2001.23, 2001.24, and 2001.25, Derivative classification, Classification marking in the electronic environment, Additional requirements, and Declassification markings; ISOO's marking guide, *Marking Classified National Security Information*; and other applicable national level policy (e.g., Atomic Energy Act for RD) for marking classified information and material.

§ 2004.40 Information system security.

(a) The responsible CSA must authorize an entity information system before the entity can use it to process classified information. The CSA must use the most complete, accurate, and trustworthy information to make a timely, credible, and risk-based decision whether to authorize an entity's system.

(b) The responsible CSA issues to entities guidance that establishes protection measures for entity information systems that process classified information. The responsible CSA must base the guidance on standards applicable to Federal systems, which must include the Federal

Information Security Modernization Act of 2014 (FISMA), P.L. 113-283, and may include National Institute of Standards and Technology (NIST) publications, Committee on National Security Systems (CNSS) publications, and Federal information processing standards (FIPS).

§ 2004.42 International programs security. [Reserved]

Appendix A to Part 2004—Acronym Table

For details on many of these terms, see the definitions at § 2004.4.

CCIPP – Classified Critical Infrastructure Protection Program

CCIPP POC – Entity point of contact under the CCIPP program

CIA – Central Intelligence Agency

CSA – Cognizant security agency

CNSS – Committee on National Security Systems

COMSEC – Communications security

CSO – Cognizant security office

DHS – Department of Homeland Security

DoD – Department of Defense

DOE – Department of Energy

EA – Executive agent (the NISP executive agent is DoD)

E.O. – Executive Order

FAR – Federal Aquisition Regulation

FOCI – Foreign ownership, control, or influence

GCA – Government contracting activity

Insider threat SO – insider threat senior official (for an agency or for an entity)

ISOO – Information Security Oversight Office of the National Archives and Records Administration (NARA)

KMO – Key managers and officials (of an entity)

LAA – Limited access authorization

NID – National interest determination

NISPOM – National Industrial Security Program Operating Manual

NRC – Nuclear Regulatory Commission

NSA – National Security Agency

ODNI – Office of the Director of National Intelligence

PA – Proxy agreement

RD – Restricted data

SF – Standard Form

SAO – Senior agency official for NISP

SAP – Special access program

SCA – Security control agreement

SCI – Sensitive compartmented information

SSA – Special security agreement

TS – Top secret (classification level)

VT – Voting trust

Dated: January 3, 2017.

David S. Ferriero

Archivist of the United States.

[FR Doc. 2017-00152 Filed: 1/10/2017 8:45 am; Publication Date: 1/11/2017]