DEPARTMENT OF DEFENSE BILLING CODE 5001-06

Office of the Secretary

32 CFR Part 117

[Docket ID: DOD-2011-OS-0063]

RIN 0790-AI71

National Industrial Security Program

AGENCY: Department of Defense (DoD).

ACTION: Interim final rule.

SUMMARY: This DoD interim final rule (rule) assigns responsibilities and establishes requirements related to the National Industrial Security Program (NISP) to ensure maximum uniformity and effectiveness for both DoD and non-DoD Components, as defined in this rule, for which the Department serves as the Cognizant Security Agency (CSA) and provides industrial security services in accordance with Executive Order (EO) 12829, "National Industrial Security Program." The rule provides guidance on the procedures used to ensure classified information will be properly safeguarded if a contractor has reported foreign ownership, control or influence (FOCI) information which DoD must evaluate, mitigate, or negate as appropriate. The rule also provides guidance for the evaluation, mitigation, and/or negation of FOCI information reported by a company, as defined in the rule, which is in process for a facility security clearance (FCL).

DATES: *Effective Date*: This rule is effective **[INSERT DATE OF PUBLICATION IN THE FEDERAL REGISTER].** Comments must be received by **[INSERT DATE 60 days from date of publication in the Federal Register]**.

ADDRESSES: You may submit comments, identified by 32 CFR part 117, Docket No. DoD-2011-OS-0063 or Regulatory Information Number (RIN) 0790-AI71 by any of the following methods:

• Federal Rulemaking Portal: http://www.regulations.gov. Follow the instructions for submitting comments.

• Mail: Federal Docket Management System Office, 4800 Mark Center Drive, 2nd floor, East Tower, Suite 02G09, Alexandria VA, 22350-3100.

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

FOR FURTHER INFORMATION CONTACT: Valerie Heil, (703) 604-1112.

SUPPLEMENTARY INFORMATION:

EXECUTIVE SUMMARY

The purpose of this part 117, subpart C is to set forth industrial security procedures and practices related to FOCI for the Components to ensure maximum uniformity and effectiveness in the DoD implementation of EO 12829.

In accordance with the authority in DoD Directive (DoDD) 5143.01, the purpose of the rule is to implement policy, assign responsibilities, establish requirements and provide procedures, consistent with EO 12829, DoD Instruction (DoDI) 5220.22, and EO 10865, “Safeguarding Classified Information within Industry,” for the protection of classified information that is disclosed to, or developed by contractors.

This rule provides NISP policy to the Components and establishes procedures concerning the initial FCL eligibility of U.S. companies that may be subject to FOCI or continued FCL eligibility for contractors subject to FOCI; provides criteria for determining whether contractors are under FOCI; prescribes responsibilities in FOCI matters; and outlines security measures that may be considered to negate or mitigate the effects of FOCI to an acceptable level. This rule does not levy requirements on U.S. contractors.

Depending upon the nature and extent of FOCI, DoD mitigates FOCI by putting into place mechanisms such as a voting trust agreement (VTA), proxy agreement (PA), special security agreement (SSA) or security control agreement (SCA). These arrangements require trustees, proxy holders or outside directors to oversee and provide business management of the U.S. contractor.

For calendar year (CY) 11, five contractors cleared by DoD were subject to a SCA, of which three required access to SECRET information and two required access to TOP SECRET information. The average number of outside directors for a SCA is two. For CY11, 16 contractors were subject to a SSA, of which 12 required access to SECRET information and four required access to TS information. The average number of outside directors for a SSA is three. In CY 11, there were no VTAs and nine PAs that required access to TS information. The average number of proxy holders for a PA is three. The proxy holders, voting trustees, or outside directors must be eligible for access at the level of the FCL.

CY 11 total estimated costs for personnel security investigations of trustees, proxy holders and outside director are as follows:

(1) The unit cost for a SECRET clearance (National Agency Check with Law and Credit NACLC) is $228

3 SCA x 2 outside directors x $228/NACLC = $1,368

12 SSA x 3 outside directors x $4005/NACLC = $8,208

(2) The unit cost for a TS (Single Scope Background Investigation – SSBI) is $4,005

2 SCAs x 3 outside directors x $4,005 = $16,020

4 SSAs x 3 outside directors x $4,005 = $48,060

9 PAs x 3 proxy holders x $4,005 = $108,135

Therefore, the total estimated investigation cost for outside directors and proxy holders under SCAs, SSAs and PAs for CY 11 is $181,791. These costs are government costs and not levied on contractors.

FOCI measures provide protection from unauthorized transfer of classified information to foreign interests, thus saving billions of dollars.

At the same time, the procedures in this rule allow companies determined to be under FOCI to be cleared through a FOCI mitigation or negation agreement and thus realize billions of dollars in classified contracts.

By maintaining the capability for foreign-owned U.S. contractors to compete for classified contracts with FOCI mitigation, DoD, through the NISP, enhances competition and realizes cost savings through that competition.

Background

DoD, as one of the four NISP CSAs, provides oversight of more than 10,000 U.S. contractors as well as another 3,000 divisions and branch offices of those contractors on behalf of the DoD Components and the non-DoD Components. Non-DoD Components issuing contracts requiring access to classified information who are not one of the four designated NISP CSAs (i.e., the Department of Energy, the Office of the Director of National Intelligence, the Nuclear

Regulatory Commission and the DoD) must enter into agreements with DOD to establish the terms of oversight on their behalf. Currently, the procedures for assessing initial FCL eligibility for U.S. companies and continued FCL eligibility for U.S. contractors which may be subject to FOCI are not uniform or consistent since these procedures do not apply to the non-DoD Components. Currently, DoD does not have uniform procedures to assess the risks and the potential adverse impact on the performance of contracts requiring access to classified information due to any FOCI information reported by U.S. contractors or U.S. companies in process for an FCL. The rule will provide uniform and effective procedures for DoD to assess the risks associated with reports of material changes to FOCI information which are submitted annually by U.S. contractors.

The rule also establishes procedures and criteria for appropriate actions to mitigate or negate any existing FOCI factors when DoD determines a U.S. company in process for an FCL or a U.S. contractor is under FOCI and is thus ineligible for access to classified information. The rule also prescribes responsibilities for FOCI matters, to include assessment of risks which may result from a contractor's FOCI information. Finally, it outlines security measures DoD may consider, implement, and oversee to mitigate or negate the effects of FOCI to an acceptable level for classified contract performance.

The addition of this rule is part of DoD's retrospective plan, completed in August 2011, under Executive Order 13563, "Improving Regulation and Regulatory Review." Executive Order 13563 emphasizes the importance of retrospective analysis of rules with its "look back" requirement, which states that "within 120 days of the date of this order, each agency shall develop…a preliminary plan" The plans should "facilitate the periodic review of rules that may be outmoded, ineffective, insufficient, or excessively burdensome, and to modify, streamline,

expand, or repeal them in accordance with what has been learned." This rule updates policy and procedures for industry that are more than 20 years old. DoD's full plan and updates can be accessed at: http://exchange.regulations.gov/exchange/topic/eo-13563.

Justification for Interim Final Rule

Without this rule, the Components face an elevated risk of unauthorized disclosure of classified information to foreign interests resulting in potential economic losses or damage to U.S. national security. There is such an increased probability of unauthorized disclosure of classified information because the owner of a U.S. company has direct authority over all aspects of his company (e.g., who gets paid, what contracts, including classified contracts are pursued, and access to information/programs that those contracts include. If the U.S. company has a foreign owner and is awarded a contract requiring access to classified information, these procedures provide actions for the USG to take to keep that foreign owner from having direct authority over the disclosure of and access to classified information. If there are no procedures as set forth in this rule to evaluate and determine how to negate or mitigate the foreign ownership, there will be nothing to prevent unauthorized disclosures of classified information since the foreign owner will have unfettered control of the U.S. company. This proposed rule provides the baseline requirements for the USG to evaluate the foreign owner's rights and determine whether those rights can be mitigated to effectively protect classified information and preclude its unauthorized disclosure. Depending upon what a foreign-owned U.S. company is working on, unauthorized disclosure of classified information could have an adverse impact on national security.

This rule allows fair and open competition among U.S. companies, including foreign-owned U.S. companies, who are vying for the opportunity to provide products and services to the Components when access to classified information is required. Also, without this rule,

Components will not have the ability to consider innovative technologies developed by foreign-owned U.S. companies due to concerns with awarding a classified contract without a uniform process to assess and effectively mitigate or negate existing FOCI. Finally, the lack of a formal, uniform process has created significant delay in the completion of National Interest Determinations (NIDs) for foreign-owned U.S. contractors. These delays increase the costs to Components by preventing contract performance when access to classified information is required.

This rule provides a baseline for protection of classified information through analysis, evaluation and, if needed, protective measures to mitigate or FOCI information at U.S. companies performing on contracts requiring access to classified information. Government Contracting Activities (GCAs) don't know if there are risks, such as foreign ownership or control of a U.S. company before awarding a contract requiring access to classified information or when a U.S. company is acquired by a foreign interest while performing on any contracts requiring access to classified information without these procedures. The uniform procedures in this rule provide the GCAs with analysis of potential adverse impact and mitigation or negation of FOCI information to allow foreign-owned U.S. companies to compete to perform on classified contracts. DoD and non-DoD Components face an increased probability of the loss or compromise of classified information and subsequent harm to the national security, as a result of the award of classified contracts to foreign-owned U.S. companies without this rule in place for the proper mitigation of FOCI information.

Definitions

For the definitions without a cited source in this rule, upon approval of this rule, those terms and their definitions will be proposed for inclusion in the next edition of the Joint Publication 1-02,

"DoD Dictionary of Military and Associated Terms" (available at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).

Regulatory Procedures

EO 12866, "Regulatory Planning and Review" and EO 13563, "Improving Regulation and Regulatory Review"

It has been certified that 32 CFR part 117 does not:

(1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a section of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities;

(2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another agency;

(3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or

(4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive Orders.

Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"

It has been certified that 32 CFR part 117 does not contain a Federal mandate that may result in expenditure by State, local and tribal governments, in aggregate, or by the private sector, of $100 million or more in any one year.

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

It has been certified that 32 CFR part 117 is not subject to the Regulatory Flexibility Act (5 U.S.C. 601) because it would not, if promulgated, have a significant economic impact on a substantial number of small entities.

Public Law 96-511, “Paperwork Reduction Act” (44 U.S.C. Chapter 35)

It has been certified that 32 CFR part 117 does not impose additional reporting or recordkeeping requirements under the Paperwork Reduction Act of 1995. Standard Form (SF) 328, “Certificate Pertaining to Foreign Interests” has been assigned OMB Control Number 0704-0194.

EO 13132, “Federalism”

It has been certified that 32 CFR part 117 does not have federalism implications, as set forth in EO 13132. This rule does not have substantial direct effects on:

(1) The States;

(2) The relationship between the National Government and the States; or

(3) The distribution of power and responsibilities among the various levels of Government.

List of Subjects in 32 CFR Part 117

Classified information, Facility security clearances, Foreign ownership, control or influence procedures, Security measures.

Accordingly, 32 CFR part 117 is added to read as follows:

PART 117-NATIONAL INDUSTRIAL SECURITY PROGRAM

Subpart A—[Reserved]

Subpart B—[Reserved]

Subpart C--Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI)

Sec.

117.55 Responsibilities.

117.56 Foreign ownership, control or influence (FOCI).

Authority: Executive Order (EO) 12829, January 6, 1993, 58 FR 3479.

Subpart A—[Reserved]

Subpart B—[Reserved]

Subpart C--Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI)

§117.51 Purpose.

This part sets forth industrial security procedures and practices related to Foreign Ownership, Control or Influence (FOCI) for the Department of Defense (DoD) Components, as defined in this part and non-DoD Components, as defined in this part, to ensure maximum uniformity and effectiveness in DoD implementation of the National Industrial Security Program (NISP) established by Executive Order (EO) 12829 “National Industrial Security Program,” (available at http://www.archives.gov/isoo/policy-documents/eo-12829.html).

§117.52 Applicability.

(a) This part applies to:

(1) The DoD Components.

(2) The non-DoD Components. When the term Government Contracting Activities (GCAs) is used, it applies to both DoD Components and non-DoD Components.

(b) This part does not:

(1) Limit in any manner the authority of the Secretary of Defense, the Secretaries of the Army, Navy and Air Force; or the Heads of the Components, as defined in this part, to grant access to classified information under the cognizance of their respective department or agency to any

individual or entity designated by them. The granting of such access is outside the scope of the NISP and is governed by Executive Order (EO) 13526, "Classified National Security Information," (available at http://www.archives.gov/isoo/pdf/cnsi-eo.pdf) and applicable disclosure policies.

(2) Limit the authority of a GCA to limit, deny, or revoke access to classified information under its statutory, regulatory, or contractual jurisdiction.

(3) Levy requirements on contractors and companies currently in process for facility security clearances (FCLs) as they are subject to the requirements of DoD 5220.22-M, "National Industrial Security Program Operating Manual (NISPOM)" (available at http://www.dtic.mil/whs/directives/corres/pdf/522022m.pdf) and the security requirements of their contracts.

§117.53 Definitions.

Unless otherwise noted, these terms and their definitions are for the purposes of this part only.

Access. As defined in DoD 5220.22-M.

Affiliate. As defined in DoD 5220.22-M.

Board resolution. A formal, written decision of a company's board of directors, used to draw attention to a single act or board decision, e.g., to approve or adopt a change to a set of rules, a new program or contract.

Carve-out. As defined in DoD Directive 5205.07, "Special Access Program (SAP) Policy," (available at http://www.dtic.mil/whs/directives/corres/pdf/520507p.pdf).

Classified contract. As defined in DoD 5220.22-M.

Classified information. As defined in Joint Publication 1-02 "DoD Dictionary of Military and Associated Terms" (available at http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf).

Company. As defined in DoD 5220.22-M.

Components. DoD Components and non-DoD Components for which DoD provides industrial security services in accordance with EO 12829.

COMSEC. As defined in Joint Publication 6-0, "Joint Communication System" (available at http://www.dtic.mil/doctrine/new_pubs/jp6_0.pdf).

Contractor. As defined in DoD 5220.22-M.

Counterintelligence. As defined in Joint Publication 1-02.

Covered transaction. As defined in DoD Instruction 2000.25, "DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)". (available at http://www.dtic.mil/whs/directives/corres/pdf/200025p.pdf)

CSA. As defined in DoD 5220.22-M.

Defense articles. As defined in DoD 5220.22-M.

Defense Industrial Base. As defined in Joint Publication 1-02.

Document. As defined in EO 13526.

DoD Components. Office of the Secretary of Defense (OSD), the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within DoD.

Facility. As defined in DoD 5220.22-M.

Facility security clearance (FCL). As defined in DoD 5220.22-M.

Facility Security Officer (FSO). A U.S. citizen contractor employee, who is cleared as one of the Key Management Personnel required for the FCL, to supervise and direct security measures necessary for implementing applicable requirements set forth in DoD 5220.22-M.

FOCI action plan. For purposes of this part, the methods or agreements that can be applied to mitigate or negate the risk of foreign ownership or control to allow a U.S. contractor to maintain or a U.S. company to be granted an FCL.

FOCI mitigation agreement. For purposes of this part, a signed agreement between a foreign interest and a U.S. contractor or a company in process for an FCL which, based on an assessment of FOCI information, imposes various security measures within an institutionalized set of company practices and procedures. Examples include board resolutions, security control agreements (SCAs) and special security agreements.

FOCI negation agreement. For purposes of this part, a signed agreement between a foreign interest and U.S. contractor or a company in process for an FCL under which the foreign owner relinquishes most ownership rights to U.S. citizens who are approved by the U.S. Government and have been favorably adjudicated for access to classified information based on the results of a personnel security clearance investigation. Examples include voting trust agreements (VTAs) and proxy agreements (PAs).

Foreign government information (FGI). As defined in EO 13526.

Foreign interest. As defined in DoD 5220.22-M.

GCA. As defined in DoD 5220.22-M.

Industrial security. As defined in DoD 5220.22-M.

Information. As defined in EO 13526.

Limited Access Authorization (LAA). As defined in DoD 5220.22-M.

National interest determination (NID). As defined in 32 CFR part 2004, “National Industrial Security Program Directive No. 1.”

Non-DoD Components. Those USG executive branch departments and agencies identified in DoD 5220.22-M that have entered into agreements with the Secretary of Defense to act as the NISP Cognizant Security Agency (CSA) for, and on their behalf, in rendering security services for the protection of classified information disclosed to or generated by industry pursuant to Section 202 of EO 12829.

Personnel security clearance (PCL). As defined in DoD 5220.22-M.

Personnel security clearance assurance (PCLSA). A written certification by USG or applicable foreign government industrial security authorities, which certifies the PCL level or eligibility for a PCL at a specified level for their citizens. The assurance is used, in the case of the United States, to give an LAA to a non-U.S. citizen, provided all other investigative requirements are met.

Prime contract. As defined in DoD 5220.22-M.

Proscribed information. TOP SECRET (TS) information, COMSEC information excluding controlled cryptographic items when unkeyed and utilized with unclassified keys, restricted data (RD), special access program (SAP) information, or sensitive compartmented information (SCI).

Restricted Data (RD). As defined in DoD 5220.22-M.

Sensitive compartmented information (SCI). As defined in Joint Publication 1-02.

Security assurance. A written confirmation, requested by and exchanged between governments, that contains the following elements: verification of the personnel security clearance (PCL) level of the sponsoring foreign government's citizens or nationals; a statement by a responsible official of the sponsoring foreign government that the recipient of the information is approved by the sponsoring foreign government for access to information of the security classification involved on behalf of the sponsoring government; and an obligation that the sponsoring foreign government will ensure compliance with any security agreement or other use, transfer and

security requirements specified by the components. The security assurance usually will be in a request for visit authorization or with courier orders or a transportation plan; but is not related to the PCL security assurance.

Special Access Program (SAP). As defined in EO 13526.

Subcontract. As defined in DoD 5220.22-M.

§117.54 Policy.

It is DoD policy that DoD FOCI procedures will be used to protect against foreign interests:

(a) Gaining unauthorized access to classified, export-controlled, or all communications security (COMSEC) (classified or unclassified) information in accordance with EO 12829 and DoD Instruction 8523.01, "Communications Security" (available at http://www.dtic.mil/whs/directives/corres/pdf/852301p.pdf). DoD FOCI procedures for access to unclassified COMSEC are set forth in National Security Agency Central Security Service (NSA/CSS) Policy Manual 3-16, "Control of Communications Security Material" (available to authorized users of SIPRNET at www.iad.nsa.smil.mil/resources/library/nsa_office_of_policy_section/pdf/NSA_CSS_MAN-3-16_080505.pdf).

(b) Adversely affecting the performance of classified contracts, in accordance with EO 12829.

(c) Undermining U.S. security and export controls, in accordance with EO 12829.

§117.55 Responsibilities.

(a) The Under Secretary of Defense for Intelligence (USD(I)) will, in accordance with DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I))" (available at http://www.dtic.mil/whs/directives/corres/pdf/514301p.pdf) and DoD Instruction 5220.22, "National Industrial Security Program" (see

http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf):

(1) Oversee policy and management of the NISP, to include FOCI matters.

(2) Direct, administer, and oversee the FOCI provisions of the NISP to ensure that the program is efficient and consistently implemented.

(3) Provide additional guidance regarding FOCI matters by memorandum as needed.

(4) Coordinate with the Under Secretary of Defense for Policy (USD(P)) and the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) on matters under their cognizance that affect the NISP consistent with paragraphs (c) and (d) of this section.

(b) The Director, Defense Security Service (DSS), in addition to the responsibilities in paragraph (d) of this section, under the authority, direction, and control of the USD(I) will in accordance with DoD Instruction 5220.22, "National Industrial Security Program" (available at http://www.dtic.mil/whs/directives/corres/pdf/522022p.pdf).

(1) Make FOCI determinations on a case-by-case basis for U.S. contractors or companies under consideration for an FCL under the NISP.

(2) Collect information necessary to examine the source, nature, and extent of a company's ownership, control, or influence by foreign interests.

(3) Determine, on behalf of the GCAs, whether a U.S. company is under FOCI to such a degree that the granting of an FCL would be inconsistent with the U.S. national security interests.

(4) Determine the security measures necessary to negate or mitigate FOCI and make recommendations to the U.S. company and to those GCAs with a contractual interest or other equity in the matter.

(5) Provide GCAs a guide to clarify their roles and responsibilities with respect to the FOCI process and to national interest determinations (NIDs), in particular. Update the guide, as

needed, in coordination with the Office of the Under Secretary of Defense for Intelligence (OUSD(I)) Security Directorate.

(6) Determine a U.S. company's eligibility for an FCL on an initial and continuing basis depending on recurring security reviews and other interactions.

(7) Develop proposed changes to maintain the currency and effectiveness of this part. Forward proposed changes and associated justification to the OUSD(I) Security Directorate for consideration as future changes to this part.

(8) Consider and, as warranted, approve requests for exception to DoD 5220.22-M in consultation with affected GCAs for specific contractors and for specific periods of time (such as, to the completion date of a contract) when a contractor is unable to comply with the requirements of DoD 5220.22-M. Consideration of such requests will include an evaluation of any proposed alternative procedures with supporting justification and coordination as applicable, consistent with paragraph (a)(4) of this section.

(9) Coordinate and receive the concurrence of the OUSD(I) Security Directorate on requests for exception to DoD 5220.22-M and consistent with paragraph (a)(4) of this section when any of the following provisions apply:

(i) The request exceeds the authority of the Director, DSS as defined in this section;

(ii) The proposed exception applies to more than one contractor location; or,

(iii) The exception would be contrary to U.S. national policy or international agreements, including those relating to foreign government information (FGI) and international issues under the cognizance of the USD(P) with coordination as applicable, consistent with paragraph (a)(4) of this section.

(c) The USD(P) will, in accordance with DoD Directive 5111.1, “Under Secretary of Defense for Policy (USD(P))” (available at http://www.dtic.mil/whs/directives/corres/pdf/511101p.pdf), advise the USD(I) and DSS on the foreign relations and international security aspects of FOCI, including FGI, foreign disclosures of U.S. classified information, exports of defense articles and technical data, security arrangements for DoD international programs, North Atlantic Treaty Organization security, and international agreements.

(d) The USD(AT&L) will, in accordance with DoD Directive 5134.01, “Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))” (available at http://www.dtic.mil/whs/directives/corres/pdf/513401p.pdf):

(1) Advise the USD(I) on the development and implementation of NISP policies, in accordance with DoD Instruction 5220.22.

(2) Ensure that DoD Components establish and maintain a record capturing the current and legitimate need for access to classified information by contractors in the Defense Industrial Base.

(3) Ensure that acquisition elements of DoD Components comply with the applicable provisions of DoD 5220.22-M.

(e) The Director, DoD SAP Central Office (SAPCO) will, in accordance with DoD Directive 5205.07, “Special Access Program (SAP) Policy” (available at http://www.dtic.mil/whs/directives/corres/pdf/520507p.pdf), notify DSS of the existence of SAP equities when DSS considers the acceptability of a contractor’s FOCI action plan. In addition, the Director, DoD SAPCO, will develop procedures for the consideration of a NID when a contractor cleared under a Special Security Agreement (SSA) requires access to an unacknowledged Special Access Program (SAP).

(f) The Heads of the Components will:

(1) Oversee compliance by GCA personnel with applicable procedures identified in this subpart.

(2) Designate in writing an individual who is authorized to make decisions and provide a coordinated GCA position on FOCI matters to DSS within timelines established in this part.

(3) Submit proposed changes to DoD 5220.22-M, as deemed appropriate, to the OUSD(I) Security Directorate.

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

(a) General. This section provides guidance for and establishes procedures concerning the initial or continued FCL eligibility of U.S. companies and U.S. contractors with foreign involvement; provides criteria for determining whether U.S. companies are under FOCI; prescribes responsibilities in FOCI matters; and outlines security measures that DSS may consider to mitigate or negate the effects of FOCI to an acceptable level. As stated in DoD 5220.22-M, and in accordance with EO 12829:

(1) The Secretary of Defense serves as the Executive Agent for inspecting and monitoring contractors who require or will require access to, or who store or will store classified information.

(2) The Components reserve the discretionary authority, and have the obligation, to impose any security procedure, safeguard, or restriction they believe necessary to ensure that unauthorized access to classified information is effectively precluded and that performance of classified contracts, as defined in DoD 5220.22-M, is not adversely affected by FOCI.

(b) Procedures. (1) Criteria. A U.S. company is considered to be under FOCI whenever a foreign interest has the power, direct or indirect (whether or not exercised, and whether or not exercisable through the ownership of the U.S. company's securities, by contractual arrangements or other means), to direct or decide matters affecting the management or operations of the

company in a manner that may result in unauthorized access to classified information or may adversely affect the performance of classified contracts.

(2) FOCI Analysis. Conducting an analysis of available information on a company to determine the existence, nature, and source of FOCI is a critical aspect of evaluating previously uncleared companies for FCLs and also in determining continued eligibility of contractors for FCLs.

(i) A U.S. company determined to be under FOCI is ineligible for an FCL unless and until security measures have been put in place to mitigate FOCI.

(ii) In making a determination as to whether a company is under FOCI, DSS will consider the information provided by the company or its parent entity on the Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests," (available at http://www.dtic.mil/whs/directives/infomgt/forms/eforms/sf0328.pdf) and any other relevant information (e.g., filings with the Securities and Exchange Commission (for publicly traded companies), articles of incorporation, by-laws, and loan and shareholder agreements, as well as other publicly available information about the company. Depending on specific circumstances (e.g., extensive minority foreign ownership at a cleared subsidiary in the corporate family), DSS may request one or more of the legal entities that make up a corporate family to submit individual SF 328s and will determine the appropriate FOCI action plan(s) that must be put in place.

(iii) When a contractor has been determined to be under FOCI, the primary consideration will be the safeguarding of classified information. DSS is responsible for taking whatever interim action is necessary to safeguard classified information, in coordination with other affected agencies as appropriate consistent with §117.54.

(iv) When a merger, sale, or acquisition involving a foreign interest and a contractor is finalized prior to having an acceptable FOCI mitigation or negation agreement in place, DSS will invalidate any existing FCL until such time as DSS determines that the contractor has submitted an acceptable FOCI action plan (see DoD 5220.22-M) and has agreed to interim measures that address FOCI concerns pending formal execution of a FOCI mitigation or negation agreement. Invalidation renders the contractor ineligible to receive new classified material or to bid on new classified contracts. If the affected GCA determines that continued access to classified material is required, DSS may continue the FCL in an invalidated status when there is no indication that classified information is at risk of compromise. If classified information remains at risk of compromise due to the FOCI, DSS will take action to impose appropriate security countermeasures or terminate the FCL, in coordination with the affected GCA.

(v) Changed conditions, such as a change in ownership, indebtedness, or a foreign intelligence threat, may justify certain adjustments to the security terms under which a contractor is cleared or, alternatively, require the use of a particular FOCI mitigation or negation agreement. Depending on specific circumstances, DSS may determine that a contractor is no longer under FOCI or, conversely, that a contractor is no longer eligible for an FCL.

(vi) If the contractor determined to be under FOCI does not have possession of classified material and does not have a current or pending requirement for access to classified information, DSS will administratively terminate the FCL.

(3) Assessing the Implications of FOCI. (i) If DSS determines that a company is under FOCI, DSS will assess the extent and manner to which the FOCI may result in unauthorized access to classified information or adverse impact on the performance of classified contracts and the type of actions, if any, that would be necessary to mitigate or negate the associated risks to a level

deemed acceptable to DSS. An analysis of some of the FOCI factors may clearly identify risk; while others may result in circumstances that would mitigate or negate risks. Therefore, these factors must be considered in the aggregate with regard to the foreign interest that is the source of the FOCI, the country or countries in which the foreign interest is domiciled and has its principal place of business (if not in the country of domicile), and any other foreign country that is identified by DSS because it is a substantial source of the revenue for, or otherwise has significant ties to, the foreign interest. DSS will consider the following FOCI factors and any other relevant information in the context of threat, vulnerability, and sensitivity of the classified information required for current or prospective contract performance when rendering a risk management assessment and determination of the acceptability of a company's FOCI action plan:

(A) Record of economic and government espionage against U.S. targets.

(B) Record of enforcement and/or engagement in unauthorized technology transfer.

(C) Record of compliance with pertinent U.S. laws, regulations, and contracts.

(D) The type and sensitivity of the information that will be accessed.

(E) The source, nature, and extent of FOCI, including, but not limited to, whether a foreign interest holds a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies of the company or prior relationships between the U.S. company and the foreign interest.

(F) The nature of any relevant bilateral and multilateral security and information exchange agreements, (e.g., the political and military relationship between the United States Government (USG) and the government of the foreign interest).

(G) Ownership or control, in whole or in part, by a foreign government.

(H) Any other factor that indicates or demonstrates a capability on the part of foreign interests to control or influence the operations or management of the business organization concerned.

(ii) As part of its FOCI assessment and evaluation of any FOCI action plan, DSS will also request and consider counterintelligence (CI) and technology transfer risk assessments and any available intelligence from all appropriate USG sources. DSS will request these assessments as soon as practicable, for the company itself and for all business entities in the company's ownership chain.

(iii) If a company disputes a DSS determination that the company is under FOCI, or disputes the DSS determination regarding the types of actions necessary to mitigate or negate the FOCI, the company may appeal in writing those determinations to the Director, DSS, for a final agency decision no later than 30 days after receipt of written notification of the DSS decision. The company must identify the specific relief sought and grounds for that relief in its appeal. In response, the Director, DSS, may request additional information from the company. At a minimum, DSS will respond to appeals within 30 days, either with a decision or an estimate as to when a decision will be rendered. DSS will not release pre-decisional information to the company, its legal counsel, or any of its representatives without the express written approval of the applicable GCAs who own the data and any other USG entities with an interest in the company's FOCI action plan.

(iv) DoD recognizes that FOCI concerns may arise in a variety of other circumstances, all of which cannot be listed in this subpart. In FOCI cases involving any foreign ownership or control, DSS will advise and consult with the appropriate GCAs, including those with special security needs, regarding the required FOCI mitigation or negation method and provide those GCAs with the details of the FOCI factors and any associated risk assessments. DSS and GCAs

will meet to discuss the FOCI action plan, when determined necessary by either DSS or the applicable GCAs. When DSS determines that a company may be ineligible for an FCL by virtue of FOCI, or that additional action by the company may be necessary to mitigate the FOCI or associated risks, DSS will promptly notify the company and require it to submit a FOCI action plan to DSS within 30 calendar days of the notification. In addition, DSS will advise company management that failure to submit the requested plan within the prescribed period of time will result in termination of FCL processing or initiation of action to revoke an existing FCL, as applicable.

(v) In instances where the identification of a foreign owner or voting interest of five percent or more cannot be adequately ascertained (e.g., the participating investors in a foreign investment or hedge fund, owning five percent or more of the company, cannot be identified), DSS may determine that the company is not eligible for an FCL.

(vi) DSS will review and consider the FOCI action plan itself, the factors identified in paragraph (b)(3)(i) of this section, and any threat or risk assessments or other relevant information. If an action plan is determined to be unacceptable, DSS can recommend and negotiate an acceptable action plan including, but not limited to, the measures identified in paragraphs (b)(4)(ii) and (b)(4)(iii) of this section. In any event, DSS will provide written feedback to a company or the company's designated representative on the acceptability of the FOCI action plan within 30 calendar days of receipt.

(4) Options to Address FOCI. (i) Under all FOCI action plans, management positions requiring PCLs in conjunction with the FCL must be filled by eligible U.S. citizens residing in the United States in accordance with DoD 5220.22-M.

(ii) When factors related to foreign control or influence are present, but unrelated to ownership, the plan must provide positive measures that assure that the foreign interest can be effectively denied access to classified information and cannot otherwise adversely affect performance on classified contracts. Non-exclusive examples of such measures include:

(A) Adoption of special board resolutions.

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

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

(D) The appointment of a technology control officer.

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

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

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

(H) Elimination or resolution of problem debt.

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

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

(iii) FOCI concerns related to foreign ownership of a company or corporate family arise when a foreign interest has the ability, either directly or indirectly, whether exercised or exercisable, to control or influence the election or appointment of one or more members to the company's governing board (e.g., Board of Directors, Board of Managers, or Board of Trustees) or its equivalent, by any means. Some methods that may be applied to mitigate the risk of foreign ownership are outlined in DoD 5220.22-M and further described in this section. While these

methods are mentioned in relation to specific ownership and control thresholds, these descriptions should not be construed as DoD-sanctioned criteria mandating the selection or acceptance of a certain FOCI action plan. DSS retains the authority to reject or modify any proposed FOCI action plan in consultation with the affected GCAs.

(A) Board Resolution. This method is often used when a foreign interest does not own voting interests sufficient to elect, or otherwise is not entitled to representation on the company's governing board. In such circumstances, the effects of foreign ownership will generally be mitigated by a resolution of the board of directors stating the company recognizes the elements of FOCI and acknowledges its continuing obligations under DD Form 441, "DoD Security Agreement" (available at http://www.dtic.mil/whs/directives/infomgt/forms/eforms/dd0441.pdf). The resolution will identify the foreign shareholders and their representatives (if any) and note the extent of foreign ownership. The resolution will also include a certification that the foreign shareholders and their representatives will not require, will not have, and can be effectively excluded from access to all classified information in the possession of the contractor, and will not be permitted to occupy positions that may enable them to influence the organization's policies and practices in the performance of classified contracts. Copies of such resolutions will be furnished to all board members and principal management officials.

(B) SCA. The SCA is a tailored FOCI mitigation agreement often used when a foreign interest does not effectively own or control a company or corporate family (i.e., the company or corporate family are under U.S. control), but the foreign interest is entitled to representation on the company's board. When an SCA is implemented, a U.S. citizen serves as an outside director, as defined in DoD 5220.22-M. DSS may determine the need for more than one outside director based on the FOCI analysis and risk assessments.

(C) SSA. The SSA is a tailored FOCI mitigation agreement that preserves the foreign owner's right to be represented on the company's board (inside directors) with a direct voice in the business management of the company while denying the foreign owner unauthorized access to classified information. An SSA is based on the analysis of the FOCI factors set forth in paragraph (b)(3) and is often used when a foreign interest effectively owns or controls a company or corporate family. DSS assesses the implications of the FOCI factors in accordance with paragraphs (b)(3) and (b)(4)(iii) of this section. U.S. citizens serve as outside directors in accordance with DoD 5220.22-M.

(1) If a GCA requires a contractor cleared under an SSA to have access to proscribed information, the GCA will initiate action to consider a NID at the pre-contract phase to confirm that disclosure of such information is consistent with the national security interests of the United States.

(2) Proscribed information includes TS; COMSEC material, excluding controlled cryptographic items when unkeyed and utilized with unclassified keys; RD; SAP; and SCI.

(3) Contractor access to proscribed information will not be granted without the approval of the agency with control jurisdiction (i.e., National Security Agency (NSA) for COMSEC, whether the COMSEC is proscribed information or not; the Office of the Director of National Intelligence (ODNI) for SCI; and the Department of Energy (DOE) for RD in accordance with its policies).

(4) In accordance with 32 CFR, part 2004 and the procedures in paragraph (b)(5) of this section, GCAs will forward a request for concurrence to NSA, ODNI, or DOE when a proposed NID involves access to COMSEC, SCI, or RD, respectively, within 30 calendar days of DSS advisement of the NID requirement. NSA, ODNI, and DOE, as appropriate, will then have 30 calendar days to render a decision.

(D) VTA or PA. These FOCI negation agreements may be used when a foreign interest effectively owns or controls a company or corporate family. Under a VTA, PA and associated documentation, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by DSS. Both FOCI agreements can effectively negate foreign ownership and control; therefore, neither agreement imposes any restrictions on the company's eligibility to have access to classified information or to compete for classified contracts including contracts with proscribed information. Both FOCI agreements can also effectively negate foreign government control (see paragraph (b)(11) of this section which provides guidance and requirements regarding foreign government ownership or control, including with respect to 10 U.S. C. 2536, "Award of Certain Contracts to Entities Controlled by a Foreign Government Prohibition (available at http://www.gpo.gov/fdsys/granule/USCODE-2010-title10/USCODE-2010-title10-subtitleA-partIV-chap148-subchapV-sec2536/content-detail.html)). DSS retains the authority to deny a proposed VTA or PA.

(iv) When DSS implements a FOCI mitigation or negation agreement at a contractor, the agreement may specify that the entire agreement, or that particular provisions of the agreement (e.g., the provisions restricting unauthorized access to classified information and unclassified export-controlled information and the provisions of the visitation policy) will apply to and will be made binding upon all present and future subsidiaries of the company. If a subsidiary requires and is eligible for an FCL at the TS level, the company executing the FOCI mitigation agreement and any intermediate parents must be formally excluded from TS access unless they have their own requirement and are otherwise eligible for TS access.

(v) DSS will provide a copy of the DSS FOCI assessment, proposed FOCI action plan and any associated risk assessments to the GCAs with an interest in the company or corporate family. In

the absence of written objections (signed at the Program Executive Office (PEO) level or higher) from GCAs with an interest in the company or corporate family, DSS may proceed with implementation of what DSS considers in its discretion to be an acceptable FOCI action plan based on available information. Unless other regulatory review processes for mergers or acquisitions have an earlier suspense date, DSS will provide a 30 calendar day period for the GCAs with an interest in the company or corporate family to provide their PEO level or higher written objections.

(vi) DSS will submit to the USD(I) for approval the DSS templates for those FOCI mitigation or negation agreements identified in paragraph (b)(4)(iii) of this section as well as templates for any supplements thereto (e.g., the electronic communications plan (ECP) or technology control plan (TCP)). DSS may propose changes to the contents of these template FOCI mitigation or negation agreements. DSS may tailor non-substantive provisions of the template agreement for any particular FOCI case without further approval from the USD(I), provided DSS notifies the OUSD(I) Security Directorate of the deviation from the template. DSS may provide this notification through the electronic submission of an annotated copy of the modified agreement.

(5) NID. The requirement for a NID to authorize access to proscribed information applies only to those foreign-owned U.S. contractors or companies in process for an FCL under an SSA which is used as a mechanism for FOCI mitigation. A NID does not authorize disclosure of classified information to a foreign government, a non-U.S. citizen or a non-U.S. entity. Timelines for NID decisions are set forth in 32 CFR part 2004 and the provisions of this paragraph. NIDs can be program, project, or contract specific, subject to the concurrence of NSA for COMSEC, ODNI for SCI or DOE for RD. For program and project NIDs, a separate NID is not required for each contract. DSS will inform the DoD SAPCO of NID requirements to

allow the SAPCO to advise of awareness of unacknowledged SAPs or any carve-out SAP activity.

(i) A NID is necessary when access to proscribed information is required for:

(A) Pre-contract activities in accordance with paragraph (b)(4)(iii)(C)(1) of this section.

(B) New contracts to be issued to a company in process for an FCL that DSS has determined to be under FOCI when an SSA is anticipated, or a contractor already cleared under an SSA.

(C) Existing contracts when a contractor is acquired by foreign interests and proposes an SSA as the FOCI action plan.

(ii) If a contractor is proposing to use an SSA to mitigate FOCI and requires access to proscribed information:

(A) DSS will:

(1) Request the contractor to provide information on all impacted contracts, both prime and subcontracts, unless the contractor is prohibited by contract from revealing their existence to DSS. In such instances, DSS will request that the contractor notify the government contracting officer and Program Security Officer of the need for a NID.

(2) Provide written notification to the individual designated by the Component, in accordance with paragraph (f) of §117.55 within 30 calendar days of identifying the requirement for a NID.

(3) Provide to appropriate GCAs the contractor's proposed FOCI action plan, any associated risk assessments, and DSS' recommendation for FOCI mitigation.

(4) Ask the GCA to identify all of the GCA's contracts affected by the proposed SSA that require a NID decision, unless the activity is unacknowledged. The cognizant SAPCO will inform the DoD SAPCO of any unacknowledged SAPs affected by the proposed SSA and consequently the NID requirement.

(5) Provide OUSD(I) Security Directorate and the OUSD(AT&L), Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, a monthly report of pending NID decisions that :

(i) Exceed 30 calendar days from the date of the DSS written notice to the applicable GCA.

(ii) Have been pending for NSA, ODNI, or DOE concurrence for more than 30 calendar days.

(B) OUSD(I) will intervene, as warranted, with GCAs regarding NID decisions pending beyond 30 calendar days from the date of the DSS written notice, as well as with NSA, ODNI, and DOE regarding concurrence decisions that remain pending beyond 30 days from the date of the GCA request.

(C) OUSD(AT&L) will confer, as warranted, with the applicable DoD Service Acquisition Executive or component equivalent about unresolved NID decisions.

(D) The GCA will, upon written notification by DSS of the need for a NID:

(1) Review the FOCI action plan proposed by the uncleared company, in addition to any associated risk assessments and the DSS analysis of the appropriate FOCI mitigation based on the existing FOCI factors.

(2) Consider the FOCI factors noted in paragraph (b)(3) of this section in the aggregate with any associated risk assessments and DSS' analysis to determine whether to issue a NID.

(3) Provide DSS, as appropriate, one of the following within 30 calendar days of the DSS written notification that a NID is required:

(i) A final, documented NID with a copy provided to the contractor. If the NID is not specific to a single program, project, or contract (e.g., a blanket NID), the GCA will also forward a copy of the NID to the OUSD(I) Security Directorate.

(ii) A copy of the GCA's request for NID concurrence sent to NSA, ODNI, or DOE, when access to COMSEC, SCI, or RD is involved. The GCA will request that NSA, ODNI, or DOE respond within 30 calendar days of the date of the GCA's written request directly to DSS with a copy to the GCA.

(iii) A GCA decision that it will not issue a NID.

(4) Contact DSS to determine an alternative method to the proposed SSA when the GCA chooses not to issue a NID (e.g., a contract modification, a contract novation, or a PA or VTA authorized by the Program Executive Officer).

(5) Notify DSS in writing when NSA, ODNI, or DOE renders a decision on a proposed NID involving access to COMSEC, SCI, or RD, respectively. A GCA's NID decision is not final until NSA, ODNI, or DOE, as applicable, respond regarding access to COMSEC, SCI, or RD.

(6) When denying a NID, retain documentation explaining the rationale for the decision.

(6) Government Security Committee (GSC). (i) Under a VTA, PA, SSA, or SCA, DSS will ensure that the contractor establishes a permanent committee of its Board of Directors or similar body known as the GSC.

(A) The members of the GSC are required in accordance with DoD 5220.22-M to ensure that the contractor maintains policies and procedures to safeguard classified and export controlled information entrusted to it, and that violations of those policies and procedures are promptly investigated and reported to the appropriate authority when it has been determined that a violation has occurred.

(B) The GSC will also take the necessary steps in accordance with DoD 5220.22-M to ensure that the contractor complies with U.S. export control laws and regulations and does not take

action deemed adverse to performance on classified contracts. This will include the appointment of a Technology Control Officer and the establishment of Technology Control Plan (TCP).

(ii) DSS will provide oversight, advice, and assistance to GSCs. These measures are intended to ensure that GSCs:

(A) Maintain policies and procedures to safeguard classified information and export-controlled unclassified information in the possession of the contractor with no adverse impact on the performance of classified contracts.

(B) Verify contractor compliance with the DD Form 441 or its successor form, the FOCI mitigation agreement or negation agreement and related documents, contract security requirements, USG export control laws, and the NISP.

(iii) In the case of an SSA, DSS will ensure that the number of outside directors exceeds the number of inside directors, as defined in DoD 5220.22-M. DSS will determine if the outside directors should be a majority of the Board of Directors based on an assessment of security risk factors pertaining to the contractor's access to classified information. In the case of an SCA, DSS will require the contractor to have at least one outside director, but may require more than one outside director based on an assessment of security risk factors.

(iv) In the case where a contractor is cleared to the SECRET level under an SSA, and also has a subsidiary with a TS FCL based on an approved NID, some or all of the outside directors of the cleared parent contractor may be sponsored for eligibility for access to TS information with their TS PCLs held by the subsidiary. Access will be at the level necessary for the outside directors to carry out their security or business responsibilities for oversight of the subsidiary company in accordance with DoD 5220.22-M. If the subsidiary has an approved NID for access to SAP or

SCI, the applicable GCA may determine that an outside director at the parent contractor requires approved access at the subsidiary.

(7) Technology Control Plans (TCPs). Under a VTA, PA, SSA, SCA, or Limited FCL, DSS will require the contractor to develop and implement a TCP as required in DoD 5220.22-M. DSS will evaluate and, if the plan is adequate, approve the TCP. The TCP must include a description of all security measures required to prevent the unauthorized disclosure of classified or export-controlled information. Although TCPs must be tailored to the specific circumstances of the contractor or corporate family to be effective, DSS may provide examples of TCPs to the contractor to assist plan creation.

(8) Electronic Communication Plan (ECP). Under a VTA, PA, or SSA, DSS will require the contractor to develop and implement an ECP tailored to the contractor's operations. DSS will determine the extent of the ECP and review the plan for adequacy. The ECP must include a detailed network description and configuration diagram that clearly delineates which networks will be shared and which will be protected from access by the foreign parent or its affiliates. The network description will address firewalls, remote administration, monitoring, maintenance, and separate e-mail servers, as appropriate.

(9) Administrative Support Agreement (ASA). There may be circumstances when the parties to a transaction propose in the FOCI action plan that the U.S. contractor provides certain services to the foreign interest, or the foreign interest provides services to the U.S. contractor. The services to be provided must be such that there is no violation of the applicable FOCI mitigation or negation agreement. If approved, the extent of such support and limitations on the support will be fully documented in an ASA.

(10) Annual Review and Certification. (i) Annual Meeting. DSS will meet at least annually with the GSCs of contractor's operating under a VTA, PA, SSA, or SCA to review and discuss the purpose and effectiveness of the FOCI mitigation or negation agreement; establish a common understanding of the operating requirements and their implementation; answer questions from the GSC members; and provide guidance on matters related to FOCI mitigation and industrial security. These meetings will also include an examination by DSS, with the participation of the (FSO) and the GSC members, of:

(A) Compliance with the approved security arrangement, standard rules, and applicable laws and regulations.

(B) Problems regarding the practical application or utility of the security arrangement.

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

(ii) Annual Certification. For contractors operating under a VTA, PA, SSA, or SCA, DSS will obtain from the Chair of the GSC an implementation and compliance report one year from the effective date of the agreement and annually thereafter. DSS will review the annual report; address, resolve, or refer issues identified in the report; document the results of this review and any follow-up actions; and keep a copy of the report and documentation of related DSS actions on file for 15 years. The GSC's annual report must include:

(A) A detailed description stating how the contractor is carrying out its obligations under the agreement.

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

(C) A detailed description of any acts of noncompliance with FOCI provisions and a discussion of steps taken to prevent such acts from recurring.

(D) Any changes or impending changes of senior management officials or key board members, including the reasons for the change.

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

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

(11) Foreign Government Ownership or Control. (i) In accordance with 10 U.S.C. 2536, the DoD cannot award contracts involving access to proscribed information to a company effectively owned or controlled by a foreign government unless a waiver has been issued by the Secretary of Defense or designee.

(ii) A waiver is not required if the company is cleared under a PA or VTA because both agreements effectively negate foreign government control.

(iii) DSS will, after consultation with the GCA, determine if a waiver is needed in accordance with subpart 209.104-1 of the Defense Federal Acquisition Regulation Supplement "Responsible Prospective Contractors, General Standards" (available at http://www.acq.osd.mil/dpap/dars/dfars/pdf/r20090115/209_1.pdf. The GCA will request the waiver from the USD(I) and provide supporting information, to include a copy of the proposed NID.

(iv) Upon receipt of an approved waiver, the GCA will forward the waiver and the NID to DSS.

(v) If the USD(I) does not grant the waiver, the company may propose to DSS an appropriate PA or VTA. Otherwise, the company is not eligible for access to proscribed information.

(12) Changed Conditions. (i) DSS will require contractors to submit timely reports of changes to FOCI by DSS-designated means in accordance with DoD 5220.22-M.

(ii) Upon receipt of changes to the SF 328 from contractors, DSS will assess the changes to determine if they are material; if they require the imposition of new FOCI mitigation or modification of existing FOCI mitigation; or if they warrant the termination of existing FOCI mitigation. DSS will periodically review the definition of material change with regard to FOCI and publish updated guidance as to what constitutes a reportable material change in coordination with OUSD(I) Security Directorate.

(13) Limited FCL. (i) A Limited FCL may be an option for a single, narrowly defined purpose when there is foreign ownership or control of a U.S. company. In that respect, a Limited FCL is similar to an LAA for a non-U.S. citizen. Consideration of a Limited FCL includes a DSS determination that the company is under FOCI and that the company is either unable or unwilling to implement FOCI negation or mitigation. A GCA or a foreign government may sponsor a Limited FCL consistent with the provisions of paragraphs (b)(13)(iii)(A) through (b)(13)(iii)(D) of this section.

(ii) DSS will:

(A) Document the requirements of each Limited FCL, including the limitations of access to classified information.

(B) Verify a Limited FCL only to the sponsoring GCA or foreign government.

(C) Ensure, in accordance with paragraph (b)(7) of this section, that the contractor has and implements a TCP consistent with DoD 5220.22-M.

(D) Process a home office along with a branch or division, when the GCA or foreign government sponsors the branch or division for a Limited FCL and ensure that the limitations of the Limited FCL are applied to the home office as well as the branch or division.

(E) Administratively terminate the Limited FCL when the FCL is no longer required.

(iii) There are four types of Limited FCLs:

(A) A GCA may sponsor a joint venture company established in the United States for the purpose of supporting a cooperative arms program involving DoD. An authorized GCA official, at the PEO level or higher, must certify in writing that the classified information to be provided to the company has been authorized for disclosure to the participating governments in compliance with U.S. National Disclosure Policy NDP-1, ""National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," (available to designated disclosure authorities on a need-to-know basis from the Office of the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff to the Under Secretary of Defense for Policy). Key management personnel (KMPs) and employees may be citizens of the countries of ownership, if DSS is able to obtain security assurances. The non-U.S. citizens retain their foreign government issued personnel security clearances. The company FSO must be a cleared U.S. citizen as set forth in DoD 5220.22-M.

(B) A U.S. subsidiary of a foreign company may be sponsored for a Limited FCL by the government of the foreign parent company when the foreign government desires to award a contract to the U.S. subsidiary involving access to classified information for which the foreign government is the original classification authority (i.e., FGI), and there is no other need for the U.S, subsidiary to have an FCL. The KMPs must all be U.S. citizens. However, if the U.S. subsidiary is to have access to U.S. classified information in the performance of the contract, the U.S. subsidiary must be considered for one of the FOCI agreements set forth in paragraph (b)(4)(iii) of this section.

(C) A foreign owned freight forwarder may be sponsored for a Limited FCL by a foreign government for the purpose of providing services only to the sponsoring government. Access to

U.S. classified information or material will be limited to information and materiel that has been authorized for export to the sponsoring government consistent with an approved direct commercial sale contract or foreign military sales letter of offer and acceptance. KMPs and employees may be citizens of the sponsoring government, if DSS is able to obtain security assurances on the individuals. As non-U.S. citizens, these individuals would not be eligible for a LAA; would be assigned under an extended visit authorization, and would retain their foreign government issued personnel security clearances. The FSO must be a U.S. citizen.

(D) A senior GCA official, consistent with paragraph (f)(3) of §117.55, may sponsor a U.S. company, determined to be under FOCI by DSS, for a Limited FCL when the other FOCI agreements described in paragraph (b)(4)(iii) and paragraphs (b)(13)(iii)(A) through (b)(13)(iii)(D) of this section do not apply, and there is a compelling need for the FCL. The official must fully describe the compelling need and certify in writing that the sponsoring GCA accepts the risk inherent in not negating or mitigating the FOCI. The Limited FCL permits performance only on a classified contract issued by the sponsoring GCA.

(14) Foreign Mergers, Acquisitions, Takeovers and CFIUS. (i) CFIUS is a USG interagency committee chaired by the Treasury Department whose purpose is to review transactions that could result in the control of a U.S. business by a foreign person in order to determine the effect of such transactions on the national security of the United States. The regulations defining the CFIUS process are at 31 CFR part 800, “Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons”.

(ii) DoD is a member of CFIUS. DoD procedures for reviewing and monitoring transactions filed with CFIUS are provided in DoD Instruction 2000.25.

(iii) The CFIUS review and the DSS industrial security review for FOCI are separate processes subject to independent authorities, with different time constraints and considerations. However, CFIUS may not mitigate national security risks that are adequately addressed by other provisions of law.

(iv) If the NISP process has not begun or has not been completed prior to the submission of a CFIUS notice, DSS will review, adjudicate, and mitigate FOCI on a priority basis. DSS will provide all relevant information to the OUSD(I) Security Directorate specifically, for any transaction undergoing concurrent CFIUS and DSS reviews.

(A) By the 10th calendar day after the CFIUS review period begins DSS will advise the OUSD (AT&L) Manufacturing and Industrial Base Policy (MIBP) CFIUS Team electronically, with a copy to the OUSD(I) Security Directorate, of the U.S. company's FCL status (e.g., no FCL, FCL in process, TS/S/C FCL).

(B) For contractors or U.S. companies in process for an FCL, DSS will provide the following input in a signed memorandum with rationale included to the Director, Security, OUSD(I) Security Directorate on or before the suspense date established by the MIBP CFIUS Team:

(1) Basic identification information about the contractor, to include name, address, and commercial and government entity code.

(2) FCL level.

(3) Identification of current classified contracts, to include identification of GCAs and any requirement for access to proscribed information.

(4) The nature and status of any discussions DSS has had with the contractor or the foreign interest regarding proposed FOCI mitigation measures.

(5) Whether DSS requires additional time beyond the established MIBP CFIUS team suspense date to determine and recommend to the OUSD(I) Security Directorate whether the proposed FOCI mitigation is sufficient to address risks within the scope of DSS's FOCI authorities.

(6) Identification of any known security issues (e.g., marginal or unsatisfactory security rating, unresolved counterintelligence concerns, alleged export violations).

(v) If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. company subject to the proposed transaction fails to comply with the FOCI reporting requirements of DoD 5220.22-M, DSS may recommend additional time through the OUSD(I) Security Directorate to resolve any national security issues related to FOCI mitigation.

(vi) If the proposed transaction involves access to proscribed information and the contractor is contemplating the use of an SSA to mitigate FOCI, the GCA will provide DSS with a preliminary determination regarding the acceptability of the proposed FOCI mitigation. The determination must be provided to DSS one day prior to the suspense date established by the MIBP CFIUS Team and must include whether a favorable NID will be provided. If the GCA does not notify DSS, DSS will not delay implementation of a FOCI action plan pending completion of a GCA's NID process as long as there is no indication that the NID will be denied.

(vii) If DSS, under its FOCI authorities, is notified of a transaction with respect to which the parties thereto have not filed a notice with CFIUS, DSS will notify the MIBP CFIUS Team through the OUSD(I) Security Directorate.

(viii) When a merger, sale, or acquisition of a contractor is finalized prior to having an acceptable FOCI mitigation agreement in place, DSS will take actions consistent with paragraph (b)(2)(iv) of this section.

DATED: April 2, 2014.

Aaron Siegel
Alternate OSD Federal Register
Liaison Officer
Department of Defense

[FR Doc. 2014-07826 Filed 04/08/2014 at 8:45 am; Publication Date: 04/09/2014]