



INTELLIGENCE

UNDER SECRETARY OF DEFENSE

5000 DEFENSE PENTAGON
WASHINGTON, D.C. 20301-5000

September 02, 2009

Incorporating Change 6, January 9, 2014

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
DEPUTY CHIEF MANAGEMENT OFFICER
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, COST ASSESSMENT AND PROGRAM
EVALUATION
DIRECTOR, NET ASSESSMENT
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DoD FIELD ACTIVITIES

SUBJECT: Directive-Type Memorandum (DTM) 09-019 - "Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)"

References: Attachment 1

Purpose. This DTM replaces policy on foreign ownership, control, or influence (FOCI) contained in section C2.2 of DoD 5220.22-R (Reference (a)) in accordance with the authority in DoD Directive 5143.01 (Reference (b)). This DTM is effective immediately. After appropriate coordination, it shall be reissued as part of Volume 3 of DoD 5220.22-M (Reference (c)) the National Industrial Security Program (NISP) Operating Manual, not later than November 30, 2014.

Applicability. This DTM applies to:

- 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 the Department of Defense (hereafter referred to collectively as the "DoD Components").

- U.S. Government (USG) departments and agencies listed in paragraph 1-103.b. of Reference (c). In accordance with section 202 of Executive Order 12829 (Reference (d)) and paragraph 3.2. of DoD Directive 5220.22 (Reference (e)), the Secretary of Defense has entered into agreements with those USG departments and agencies for the purpose of rendering industrial security services. In these agreements, the head of the USG department or agency agrees to comply with the provisions of Reference (a) and changes thereto, such as this DTM. DoD Components and these non-DoD agencies are collectively referred to as “Government Contracting Activities” (GCAs) within this interim guidance.
- This DTM does not levy requirements on companies. Cleared companies and companies in process for facility security clearance are subject to the requirements of Reference (c) and other security requirements of their contracts.
- Nothing contained in this DTM shall affect the authority of a GCA to limit, deny, or revoke access to classified information under its statutory, regulatory, or contractual jurisdiction.

Policy. It is DoD policy that:

- The Department of Defense shall allow foreign investment consistent with the national security interests of the United States.
- DoD FOCI procedures shall be used to protect against foreign interests:
1) gaining unauthorized access to classified, all Communications Security (COMSEC) (classified or unclassified), or export-controlled information; 2) adversely affecting the performance of classified contracts; or
3) undermining U.S. security and export controls.

Responsibilities

- The Under Secretary of Defense for Intelligence (USD(I)) shall oversee policy and management of the National Industrial Security Program (NISP), to include FOCI matters.
- The Director, Defense Security Service (DSS), under the authority, direction, and control of the USD(I), shall make FOCI determinations for U.S. companies cleared or under consideration for a facility clearance (FCL) under the NISP. The Director, DSS, may delegate this responsibility

within DSS. FOCI determinations shall be made on a case-by-case basis. In this regard, the Director, DSS, shall:

- Collect information necessary to examine the source, nature, and extent of a company's ownership, control, or influence by foreign interests.
 - 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 national interest.
 - Determine the security measures necessary to mitigate FOCI and make recommendations to the U.S. company and to those GCAs with an official interest in the matter.
 - Determine, initially and on a continuing basis, the U.S. company's eligibility for an FCL.
- The Heads of the GCAs shall ensure GCA compliance with applicable procedures identified in this DTM.

Procedures. Attachment 2 provides procedures for complying with this DTM.

Releasability. UNLIMITED. This DTM is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.


James R. Clapper, Jr.

Attachments:
As stated

ATTACHMENT 1

REFERENCES

- (a) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985
- (b) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence (USD(I)),
November 23, 2005
- (c) DoD 5220.22-M, "National Industrial Security Program Operating Manual,"
February 28, 2006
- (d) Executive Order 12829, "National Industrial Security Program," January 6, 1993, as
amended
- (e) DoD Directive 5220.22, "National Industrial Security Program,"
September 27, 2004
- (f) Section 2536 of Title 10, United States Code
- (g) Subpart 209.104-1 of the Defense Federal Acquisition Regulation Supplement
(DFARS), as amended
- (h) Section 2170 of Title 50, United States Code Appendix, as amended

ATTACHMENT 2

FOCI PROCEDURES

1. GENERAL. This attachment provides guidance for and establishes procedures concerning the initial or continued FCL eligibility of U.S. companies with foreign involvement; provides criteria for determining whether U.S. companies are under FOCI; prescribes responsibilities in FOCI matters; and outlines security measures that may be considered to mitigate the effects of FOCI to an acceptable level. As stated in Reference (c), and in accordance with Reference (d):

a. The Secretary of Defense serves as the USG Executive Agent for inspecting and monitoring the contractors, licensees, and grantees who require or will require access to, or who store or will store classified information.

b. The USG reserves the discretionary authority, and has the obligation, to impose unilaterally any security method, safeguard, or restriction it believes necessary to ensure that unauthorized access to classified information is effectively precluded and that performance of classified contracts, as defined in Reference (c), is not adversely affected by FOCI.

2. PROCEDURES

a. 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.

b. FOCI Analysis. FOCI analysis is a critical aspect of evaluating previously uncleared companies for FCLs and also in determining continuing eligibility of currently cleared companies for FCLs.

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

(2) In making a determination as to whether a company is under FOCI, DSS shall consider the information provided by the cleared company or its parent entity on the Standard Form (SF) 328, "Certificate Pertaining to Foreign Interests," and any

other relevant information. 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 mitigation instrument(s) that must be put in place.

(3) When a company has been determined to be under FOCI, the primary consideration shall 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.

(4) When a merger, sale, or acquisition involving a cleared U.S. company is finalized prior to having an acceptable mitigation agreement in place, DSS shall invalidate any existing FCL until such time as DSS determines that the company has submitted an acceptable FOCI action plan in accordance with paragraph 2-303. of Reference (c). Invalidation renders the company ineligible to receive new classified material or to bid on new classified contracts. However, if the affected GCA determines that continued access to classified material is required, DSS may continue the FCL so long as there is no indication that classified information is at risk of compromise. If there is any concern that classified information is at risk of compromise due to the FOCI and security measures cannot be taken to remove the possibility of unauthorized access to classified information, DSS shall take action to terminate the FCL.

(5) Changed conditions, such as a change in ownership, indebtedness, or the foreign intelligence threat, may justify certain adjustments to the security terms under which a company is cleared or, alternatively, require the use of a particular FOCI mitigation arrangement. If a changed condition is of sufficient significance, it might also result in a determination that a company is no longer considered to be under FOCI or that a company is no longer eligible for an FCL because FOCI is not, or cannot be, in the view of DSS, appropriately mitigated.

(6) If the company 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 shall administratively terminate the FCL.

c. Determining the Appropriate FOCI Mitigation Measures

(1) If DSS determines that a company is under FOCI, DSS shall determine the extent and manner to which the FOCI may result in unauthorized access to classified information and the type of actions, if any, that would be necessary to mitigate the associated risks to a level deemed acceptable to DSS. 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 shall consider:

(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 shall be accessed.

(e) The source, nature, and extent of FOCI, including, but not limited to, whether foreign persons hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies of the company.

(f) The nature of any bilateral and multilateral security and information exchange agreements that may pertain.

(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.

(2) As part of its FOCI assessment and evaluation of any mitigation plan, DSS shall also obtain and consider counterintelligence and technology transfer risk assessments from all appropriate USG sources. DSS shall request the assessments as soon as practicable, for the cleared company itself and for all business entities in the company's ownership chain.

(3) 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 the FOCI, the company may appeal in writing those determinations to the Director, DSS, for a final agency decision no later than 30 calendar 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. The Director, DSS, may request

additional information from the company to make a final decision. DSS shall respond to appeals within 30 calendar days, either with a decision or an estimate as to when a decision will be rendered.

d. FOCI Action Plans

(1) The Department of Defense recognizes that foreign ownership concerns may arise in a variety of other circumstances, all of which cannot be listed here. In FOCI cases involving foreign ownership, DSS shall advise and consult with the appropriate GCAs, including those with special security needs, regarding the required mitigation method. 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 shall promptly notify the company and require it to submit a FOCI action plan to DSS within 30 calendar days of the notification. In addition, company management shall be advised that failure to submit the requested plan within the prescribed period of time will result in termination of FCL processing action or initiation of action to revoke an existing FCL, as applicable.

(2) In instances where the identification of a foreign owner cannot be adequately ascertained (e.g., the participating investors in a foreign investment or hedge fund cannot be identified), DSS may make a determination that the company is not eligible for an FCL.

(3) DSS shall review the acceptability of the FOCI action plan submitted by a company. DSS shall consider the FOCI action plan itself, the factors identified in paragraph 2.c.(1) of this attachment, and any threat or risk assessments or other relevant information received by DSS. If an action plan is determined to be unacceptable, DSS is authorized to recommend and negotiate an acceptable action plan including but not limited to the measures identified in paragraphs 2.d.(4) and 2.d.(5) of this attachment.

(4) When factors related to foreign control or influence are present, but not those related 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. In accordance with paragraph 2-302.c. of Reference (c), 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 company component performing on classified contracts.
- (j) Other actions that negate or mitigate foreign control or influence.

(5) 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 described in paragraph 2-303. of Reference (c). While these methods are mentioned in relation to specific ownership and control thresholds, they should not be interpreted as DoD policy to pre-determine or select a certain mitigation plan without regard for the overall risk assessment.

(a) Board Resolution, 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 ordinarily be mitigated by a resolution of the board of directors whereby the cleared firm recognizes the elements of FOCI and acknowledges its continuing obligations under DD Form 441, "Department of Defense Security Agreement." The resolution shall identify the foreign shareholders and their representatives, if any, and note the extent of foreign ownership, including 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 cleared facility, 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 shall be furnished to all board members and principal management officials.

(b) Security Control Agreement (SCA), when a foreign interest does not effectively own or control a company or corporate family but is entitled to representation on the company's board. U.S. citizen(s) will serve as Outside Director(s), as defined in paragraph 2-305. of Reference (c).

(c) Special Security Agreement (SSA), when a foreign interest effectively owns or controls a company or corporate family. If a GCA requires a company cleared under an SSA to have access to proscribed information, the GCA shall be required to complete a NID to confirm that disclosure of such information will not harm the national security interests of the United States. U.S. citizens will serve as Outside Directors. Proscribed information includes Top Secret (TS); COMSEC material, excluding controlled cryptographic items when unkeyed or utilized with unclassified keys; Restricted Data (RD); Special Access Program (SAP); and Sensitive Compartmented Information (SCI). Access to the proscribed information in this subparagraph shall not be granted without the approval of the agency with control jurisdiction (e.g., 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.

(d) Voting Trust or Proxy Agreement, when a foreign interest effectively owns or controls a company or corporate family. Under either the Voting Trust or Proxy Agreement arrangement, the foreign owner relinquishes most rights associated with ownership of the company to cleared U.S. citizens approved by the USG. Under a Voting Trust Agreement, the foreign owner transfers legal title in the company to the trustees. Under a Proxy Agreement, the foreign owner's voting rights are conveyed to the proxy holders. Neither arrangement imposes any restrictions on the company's eligibility to have access to classified information or to compete for classified contracts. Both arrangements can effectively negate foreign ownership and control and for purposes of section 2536 of title 10, United States Code (Reference (f)), both arrangements can also effectively negate foreign government control (see paragraph 2.f. of this attachment). DSS reserves the discretion to deny a proposed Voting Trust or Proxy Agreement.

(6) Under all methods of FOCI mitigation, management positions requiring personnel security clearances in conjunction with the FCL must be filled by eligible U.S. citizens residing in the United States.

(7) When a FOCI mitigation agreement is put in place at a cleared company, 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) shall apply to and shall 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.

(8) DSS shall provide a copy of the DSS FOCI assessment and proposed FOCI mitigation plan to the GCAs with an interest in the company or corporate family. In the absence of written objections (signed at the Program Executive Office 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 mitigation plan based on available information.

(9) The USD(I) will approve templates for those FOCI mitigation agreements identified in paragraph 2.d.(5) of this attachment. DSS may propose changes to the contents of these template FOCI mitigation 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 Security Directorate, Office of the USD(I) (hereafter referred to as the OUSD(I) Security Directorate) of the deviation from the template.

e. NID. The requirement for NIDs applies equally to new contracts to be issued to companies already cleared under SSAs as well as existing contracts when cleared companies are acquired by foreign interests and an SSA is the proposed mitigation. Upon notification from DSS of the pending merger or acquisition by a foreign interest of a cleared company performing on a contract that requires access to proscribed information, or other transaction or event that would cause the cleared company to be under FOCI, the GCA shall review the FOCI action plan proposed by the company. If the company is proposing to use an SSA to mitigate FOCI, DSS shall advise the GCA of the need for a NID, and the GCA shall determine whether a favorable NID will be issued. (See paragraph 2.c.(1) of this attachment for FOCI factors which a GCA may consider when contemplating a NID.) If the GCA determines that a favorable NID is not warranted, the GCA shall contact DSS to address the acceptability of the proposed SSA as a means to mitigate FOCI.

(1) NIDs can be program, project, or contract specific. For program and project NIDs, a separate NID is not required for each contract. DSS may require the GCA to identify all contracts affected by the NID. The NID decision shall be made at the GCA's Program Executive Office level.

(2) The GCA shall provide the NID to DSS. If the NID is not specific to a single program, project, or contract (i.e., a blanket NID), the GCA shall also forward a copy of the NID to the OUSD(I) Security Directorate.

(3) If the proscribed information is under the classification or control jurisdiction of a USG department or agency other than the GCA (e.g., NSA for COMSEC, the ODNI for SCI, and the DOE for RD), the GCA shall advise that USG department or agency that its written concurrence is required before the GCA may issue a NID. The GCA shall forward the completed NID and any required concurrences to DSS.

(4) DSS shall not delay implementation of a FOCI action plan pending completion of a GCA's NID process as long as there is no indication that a NID will be denied. However, the company shall not have access to additional proscribed information until the GCA issues the NID.

(5) DSS shall not take action on a company's request to upgrade an existing SSA FCL to TS without a NID covering the prospective TS access.

f. Foreign Government Ownership or Control

(1) In accordance with Reference (f), the Department of Defense 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 as specified in paragraph 2.f.(3) of this attachment.

(2) A waiver is not required if a Proxy or Voting Trust Agreement is approved by DSS.

(3) The GCA shall determine, after consultation with DSS, if a waiver is needed in accordance with subpart 209.104-1 of the Defense Federal Acquisition Regulation Supplement (DFARS) (Reference (g)), and shall request the waiver from the USD(I). The GCA shall provide the USD(I) with supporting information, if requested by the USD(I) or designee. The GCA shall also forward a copy of the NID to the OUSD(I) Security Directorate.

(4) Upon receipt of the waiver, if issued, the GCA shall forward the approved waiver and the NID to DSS.

(5) If the USD(I) does not grant the waiver, the company may propose to DSS an appropriate Proxy or Voting Trust Agreement. Otherwise the company is not eligible for access to proscribed information.

g. Government Security Committee (GSC)

(1) Under a Voting Trust Agreement, Proxy Agreement, SSA, or SCA, DSS shall ensure that the cleared company establishes a permanent committee of its Board of Directors or similar body known as the GSC.

(2) DSS shall take measures to ensure that, in every case where a GSC is established as part of a FOCI mitigation measure, the GSC:

(a) Maintains policies and procedures to safeguard classified information and export-controlled unclassified information in the possession of the company.

(b) Ensures that the company complies with the DD Form 441 or its successor form, the FOCI mitigation agreement, applicable contract provisions regarding security, USG export control laws, and the NISP.

(3) In the case of an SSA, the number of Outside Directors must exceed the number of Inside Directors, defined in paragraph 2-303.c. of Reference (c). DSS shall 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 company's access to classified information. In the case of an SCA, DSS shall require the company to have at least one Outside Director. DSS may require more than one Outside Director for an SCA based on an assessment of security risk factors pertaining to the company's access to classified information.

(4) In the case where a company operating under an SSA is the parent of a company that has been provided access, pursuant to a NID or otherwise, to proscribed information by a GCA, some or all of the Outside Directors at the cleared parent company may be sponsored for eligibility for access to classified information. Access shall be at the level necessary for the Outside Director(s) to carry out their security or business responsibilities for oversight of the subsidiary company in accordance with Reference (c).

h. Technology Control Plans (TCPs). Under a Voting Trust, Proxy Agreement, SSA, or SCA, DSS will require the company to develop and implement a TCP. DSS shall be responsible for approving the TCP. The TCP must include a description of all security measures determined to be necessary to prevent the unauthorized disclosure of classified or export-controlled information. Although TCPs must be tailored to the specific circumstances of the company or corporate family to be effective, DSS may provide examples of TCPs for use by the company in creating its own plan.

i. Electronic Communications Plan (ECP). Under a Voting Trust, Proxy Agreement, SSA, or SCA, DSS will require the company to develop and implement an ECP applicable to the company's operations. DSS shall determine the needed extent of, and approve, the ECP. 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 foreign access. The network description shall address firewalls,

remote administration, monitoring, maintenance, and separate e-mail servers, as appropriate.

j. Annual Review and Certification

(1) Annual Meeting. DSS shall meet at least annually with the GSCs of companies operating under a Voting Trust Agreement, Proxy Agreement, SSA, or SCA to review and discuss the purpose and effectiveness of the FOCI mitigation and other security arrangements; establish 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 shall also include an examination by DSS, with the participation of the Facility Security Officer and the GSC members, of:

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

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

(c) Questions as to whether security controls, practices, or procedures warrant adjustment.

(2) Annual Certification. For companies operating under a Voting Trust Agreement, Proxy Agreement, SSA, or SCA, DSS shall obtain from the Chair of the GSC an implementation and compliance report 1 year from the effective date of the agreement (and annually thereafter). DSS shall review the annual report; address, resolve, or refer, as appropriate, 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 report must include:

(a) A detailed description of the manner in which the company 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, whether inadvertent or intentional, with a discussion of steps that were 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.

k. Changed Conditions

(1) DSS shall require that companies submit timely reports of changes to FOCI by DSS-designated means.

(2) Upon receipt of changes to the SF 328 from companies, DSS shall assess the changes to determine if they are material; if they require the imposition of FOCI mitigation where none existed before or modification of existing FOCI mitigation; or if they necessitate the termination of existing FOCI mitigation.

1. Limited FCL. Upon receipt of a request from a GCA, in accordance with paragraph 2-309. of Reference (c), DSS may issue a Limited FCL to a foreign owned company when FOCI mitigation is not feasible. A company that is issued a Limited FCL will normally not be required to have any FOCI mitigation measures in place, but is required to meet other provisions of Reference (c) on the protection of classified and export-controlled information. A Limited FCL may be granted under one of two conditions:

(1) The government of the foreign country from which the foreign ownership of the company is derived and the United States have entered into an Industrial Security Agreement, and the classified information to be disclosed to the company has been authorized for release to that foreign government in conformity with the U.S. National Disclosure Policy. Key management personnel (KMP) may be citizens of the country of ownership, if DSS is able to obtain a security assurance (i.e., assurance from the government of the country of citizenship that a KMP is eligible for access to classified information).

(2) An authorized official of the GCA certifies in writing that there is a compelling need to issue the Limited FCL and accepts the risk inherent in not mitigating the FOCI. The Limited FCL permits performance only on classified contracts issued by the GCA that sponsored the company for the Limited FCL. DSS shall verify a Limited FCL only to the sponsoring GCA.

m. Foreign Mergers, Acquisitions, and Takeovers and the Committee on Foreign Investment in the United States (CFIUS)

(1) The CFIUS, an interagency committee chaired by the Secretary of the Treasury, conducts reviews of proposed mergers, acquisitions, and takeovers of U.S. persons (i.e., any form of business entity) by foreign persons under section 721 of the Defense Production Act of 1950, section 2170 of title 50, United States Code Appendix, as amended (Reference (h)). A CFIUS review is a voluntary process that is normally initiated by companies involved in the transaction. During the review process, foreign and U.S. persons submit the transaction for review to CFIUS so that its impact on U.S. national security can be assessed by CFIUS member agencies.

(2) The process of reviewing any given acquisition involves several steps. Upon accepting a jointly filed notice of a covered transaction, CFIUS conducts an initial 30 calendar day review to determine whether the transaction presents national security considerations that warrant a full-scale second-stage investigation. If CFIUS determines that the transaction does not pose such concerns, the process ends with a determination notice to the parties that action pursuant to Reference (h) is concluded. If CFIUS determines that the acquisition may pose national security concerns, the review process continues with a 45 calendar day second-stage investigation period. If the transaction involves foreign government control of the acquired U.S. entity, the review automatically proceeds to the second-stage investigation unless CFIUS determines during the 30 calendar day review that the transaction does not impair U.S. national security. If concerns cannot be resolved, CFIUS member agencies may recommend to the President that the transaction be suspended or prohibited. The President then has 15 calendar days to decide what action to take, if any.

(3) The CFIUS review and the DSS industrial security review for FOCI are carried out in two parallel but separate processes with different time constraints and considerations. DSS shall review, adjudicate, and mitigate FOCI for companies that are also under CFIUS review on a priority basis and shall forward all relevant information to the OUSD(I) Security Directorate for a consolidated reply to the DoD CFIUS representative as follows:

(a) For any CFIUS transaction about which DSS is notified, by the tenth calendar day after the CFIUS filing DSS will advise Defense Technology Security Administration (DTSA) electronically, with a copy to the OUSD(I) Security Directorate, of the company's FCL status (e.g., no FCL, FCL in process, TS/Secret/Confidential FCL).

(b) If the company is cleared or in process for an FCL, DSS input is critical to the process of defining a DoD position on the CFIUS case. Therefore, for cleared and in-process companies, DSS will provide their input to the OUSD(I) Security Directorate on or before the DTSA-established suspense date for all DoD Components to submit their positions on the proposed transaction. DSS shall include:

1. Basic identification information for the cleared company, to include name, address, and commercial and government entity (CAGE) 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 cleared company or the foreign interest regarding proposed FOCI mitigation measures.

5. The DSS position regarding further CFIUS investigation (stated in a signed memorandum with rationale, if DSS is recommending further investigation).

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

(4) If a transaction under CFIUS review would require consummation of new FOCI mitigation measures, DSS shall promptly advise the parties to the transaction and request that they submit to DSS a plan to mitigate FOCI.

(a) If it appears that an agreement cannot be reached on material terms of a FOCI action plan, or if the U.S. party to the proposed transaction fails to comply with the FOCI reporting requirements of Reference (c), DSS may recommend through the OUSD(I) Security Directorate a 45 calendar day investigation of the transaction to determine the effects on national security and to decide whether to recommend that the President take any action.

(b) If the proposed transaction involves access to proscribed information and the company is contemplating the use of an SSA to mitigate FOCI, the GCA shall provide DSS with a preliminary determination, 1 day prior to the due date assigned to the CFIUS filing by DTSA, as to whether a favorable NID will be provided. If the GCA does not notify DSS, DSS shall 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 shall be denied.

(5) If DSS becomes aware of a proposed transaction that should be reviewed by CFIUS, and the parties thereto do not file a joint voluntary notice with CFIUS to initiate review within a reasonable time, DSS shall notify DTSA through the OUSD(I) Security Directorate.

(6) When a merger, sale, or acquisition is finalized prior to having an acceptable mitigation agreement in place, DSS shall invalidate the existing FCL until such time as DSS determines that the company has submitted an acceptable FOCI action plan in accordance with paragraph 2-303 of Reference (c).