Department of Defense
MANUAL

NUMBER 5220.32, Volume 2
April 17, 2014
Incorporating Change 2, Effective December 10, 2021

USD(I&S)

SUBJECT: National Industrial Security Program: Procedures for Government Activities Relating to Foreign Ownership, Control, or Influence (FOCI)

References: See Enclosure 1

1. PURPOSE

a. Manual. This Manual is composed of several volumes, each containing its own purpose. In accordance with the authority in DoD Directive (DoDD) 5143.01 (Reference (a)), the purpose of the overall manual is to implement policy, assign responsibilities, establish requirements, and provide procedures, consistent with Executive Order 12829 (Reference (b)), DoD Instruction (DoDI) 5220.22 (Reference (c)), and Executive Order 10865 (Reference (d)), for the protection of classified information that is disclosed to, or developed by contractors, licensees, and grantees of the U.S. Government (USG).

b. Volume. This Volume:

(1) Sets forth industrial security procedures and practices related to FOCI for Department of Defense (DoD) and non-DoD agencies, who have entered into agreements with DoD to act on their behalf to provide industrial security services in accordance with Reference (b) (hereinafter referred to collectively as "components") to ensure maximum uniformity and effectiveness in DoD implementation of the National Industrial Security Program (NISP) in accordance with Reference (b).

(2) Cancels Directive-Type Memorandum 09-019 (Reference (e)), Under Secretary of Defense for Intelligence Memorandum (Reference (f)), and Deputy Secretary of Defense Memorandum (Reference (g)).

(3) Cancels section C2.2 of DoD 5220.22-R (Reference (h)).

2. APPLICABILITY. This Volume:

a. Applies to:

(1) 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 (hereinafter referred to collectively as the "DoD Components").

(2) Those non-DoD executive branch departments and agencies (hereinafter referred to collectively as the "non-DoD Components") that have entered into agreements with the Secretary of Defense, under which DoD acts as the cognizant security agency (CSA), to provide security oversight services to ensure the protection of classified information disclosed to or generated by contractors, licensees and grantees (hereinafter referred to as contractors). When the term Government Contracting Activities (GCAs) is used, it applies to both DoD and non-DoD Components.

b. 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 GCAs 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 13526 (Reference (i)) 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 Part 117 of Title 32, Code of Federal Regulations (Reference (j)) and the security requirements of their contracts.

3. DEFINITIONS. See Glossary.

4. 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 Reference (b) and DoDI 8523.01 (Reference (k)). DoD FOCI procedures for access to unclassified COMSEC are located in National Security Agency Central Security Service (NSA/CSS) Policy Manual 3-16 (Reference (l)).

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

c. Undermining U.S. security and export controls, in accordance with Reference (b).

5. RESPONSIBILITIES. See Enclosure 2.

6. PROCEDURES. See Enclosure 3.

7. RELEASABILITY. Cleared for public release. This volume is available on the Directives Division Website at https://www.esd.whs.mil/DD/.

8. SUMMARY OF CHANGE 2. In accordance with the November 30, 2021 Office of the Under Secretary of Defense for Intelligence and Security memorandum (Reference (y)), this administrative change:

a. Renumbers the issuance.

b. Updates references to DoD 5220.22-M, also known as the National Industrial Security Program Operating Manual (NISPOM). The NISPOM became Part 117 of Title 32, Code of Federal Regulations, and the DoD issuance was subsequently cancelled.

9. EFFECTIVE DATE. This volume is effective April 17, 2014.

Michael G. Vickers
Under Secretary of Defense
for Intelligence

Enclosures
1. References
2. Responsibilities
3. FOCI Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1

REFERENCES

(a) DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended
(b) Executive Order 12829, "National Industrial Security Program," January 6, 1993, as amended
(c) DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011, as amended
(d) Executive Order 10865, "Safeguarding Classified Information Within Industry," February 20, 1960, as amended
(e) Directive-Type Memorandum (DTM) 09-019, "Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)," September 2, 2009 (hereby cancelled)
(f) Under Secretary of Defense for Intelligence Memorandum, "Improving Implementation of Directive-Type Memorandum 09-019, 'Policy Guidance for Foreign Ownership, Control or Influence (FOCI),'" October 29, 2010 (hereby cancelled)
(g) Deputy Secretary of Defense Memorandum, "Improving Implementation of Foreign Ownership, Control or Influence (FOCI)," September 14, 2011 (hereby cancelled)
(h) DoD 5220.22-R, "Industrial Security Regulation," December 4, 1985
(i) Executive Order 13526, "Classified National Security Information," December 29, 2009
(j) Part 117 of Title 32, Code of Federal Regulations, also known as the National Industrial Security Program Operating Manual (NISPOM)
(k) DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008
(l) National Security Agency Central Security Service (NSA/CSS) Policy Manual 3-16, "Control of Communications Security (COMSEC) Material," August 5, 2005[1]
(m) DoD Instruction 5025.01, "DoD Issuances Program," August 1, 2016, as amended
(n) DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020
(o) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended
(p) DoD Directive 5205.07, "Special Access Program (SAP) Policy," July 1, 2010, as amended
(q) Part 2004 of Title 32, Code of Federal Regulations
(r) Section 2536 of Title 10, United States Code
(s) Department of Defense Federal Acquisition Regulation Supplement (DFARS), current edition
(t) National Disclosure Policy-1, "National Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations," October 1, 1988[2]
(u) Part 800 of Title 31, Code of Federal Regulations

[1] Copy is 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
[2] Provided 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

(v) DoD Instruction 2000.25, "DoD Procedures for Reviewing and Monitoring Transactions Filed With the Committee on Foreign Investment in the United States (CFIUS)," August 5, 2010, as amended
(w) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition
(x) Joint Publication 6-0, "Joint Communications System," June 10, 2010
(y) Office of the Under Secretary of Defense for Intelligence and Security, "Approval to Cancel Department of Defense 5220.22-M, "National Industrial Security Program Operating Manual," and Summary of Changes," November 30, 2021

ENCLOSURE 2

RESPONSIBILITIES

1. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)). The USD(I&S) will, in accordance with References (a) and (c):

a. Oversee policy and management of the NISP, to include FOCI matters.

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

c. Provide additional guidance regarding FOCI matters by memorandum as needed.

d. 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 sections 3 and 4 of this enclosure.

2. DIRECTOR, DEFENSE SECURITY SERVICE (DSS). In addition to the responsibilities in section 6 of this enclosure, the Director, DSS, under the authority, direction, and control of the USD(I&S), will, in accordance with Reference (c):

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

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

c. 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.

d. 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.

e. 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 and Security, Security Policy and Oversight Division (OUSD(I&S) SPOD).

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

g. Develop proposed changes to maintain the currency and effectiveness of this Volume in accordance with Reference (m). Forward proposed changes and associated justification to the OUSD(I&S) SPOD for consideration as future changes to this Volume.

h. Consider and, as warranted, approve requests for exception to Reference (j) 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 Reference (j) requirements. Consideration of such requests will include an evaluation of any proposed alternative procedures with supporting justification and coordination as applicable, consistent with paragraph 1.d. of this enclosure.

i. Coordinate and receive the concurrence of the OUSD(I&S) SPOD on requests for exception to Reference (j) and consistent with paragraph 1.d. of this enclosure when any of the following provisions apply:

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

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

(3) 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 1.d. of this enclosure.

3. USD(P). The USD(P) will, in accordance with DoDD 5111.01 (Reference (n)), advise the USD(I&S) 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.

4. USD(AT&L). The USD(AT&L) will, in accordance with DoDD 5134.01 (Reference (o):

a. Advise the USD(I&S) on the development and implementation of NISP policies, in accordance with Reference (c).

b. 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.

c. Ensure that acquisition elements of DoD Components comply with the applicable provisions of this Manual.

5. DIRECTOR, DoD SPECIAL ACCESS PROGRAM CENTRAL OFFICE (SAPCO). The Director, DoD SAPCO, will, in accordance with DoDD 5205.07 (Reference (p)), 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).

6. HEADS OF THE COMPONENTS. The Heads of the components will:

a. Oversee compliance by GCA personnel with applicable procedures identified in this Volume.

b. 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 Volume.

c. Submit proposed changes to this Volume, as deemed appropriate, to the OUSD(I&S) SPOD.

ENCLOSURE 3

FOCI PROCEDURES

1. GENERAL. This enclosure 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 Reference (j), and in accordance with Reference (b):

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

b. 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 is not adversely affected by FOCI.

2. AMENDMENT OF VOLUME. Amendment of this Volume must be processed in accordance with Reference (m).

3. 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. 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.

(1) 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.

(2) 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," 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.

(3) 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 section 4 above the signature of this Volume.

(4) 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 Reference (j)) 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.

(5) 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.

(6) 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.

c. Assessing the Implications of FOCI

(1) 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 identity 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 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.

(2) 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.

(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 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.

(4) DoD recognizes that FOCI concerns may arise in a variety of other circumstances, all of which cannot be listed within this Volume. 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.

(5) 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.

(6) DSS will review and consider the FOCI action plan itself, the factors identified in subparagraph 3.c.(1) of this enclosure, 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 subparagraphs 3.d.(2) and 3.d.(3) of this enclosure. 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.

d. Options to Address FOCI

(1) Under all FOCI action plans, management positions requiring personnel security clearances (PCLs) in conjunction with the FCL must be filled by eligible U.S. citizens residing in the United States in accordance with Reference (j).

(2) 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.

(3) 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 Reference (j) 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". 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) Security Control Agreement (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. 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 3.c. of this enclosure 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 3.c. and 3.d.(3) of this enclosure. U.S. citizens will serve as outside directors in accordance with Reference (j).

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 TOP SECRET (t); COMSEC material, excluding controlled cryptographic items when unkeyed and utilized with unclassified keys; Restricted Data (RD); SAP; and sensitive compartmented information (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 part 2004 of title 32, Code of Federal Regulations (Reference (q)) and the procedures in paragraph 3.e. of this enclosure, GCAs will forward a request for concurrence to NSA, ODNI, or DOE when a proposed NID involves access 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 their decision.

(d) Voting Trust Agreement (VTA) or Proxy Agreement (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 3.k. of this enclosure, which provides guidance and requirements regarding foreign government ownership or control, including with respect to section 2536 of title 10, United States Code (Reference (r)). DSS retains the authority to deny a proposed VTA or PA.

(4) 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.

(5) 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.

(6) DSS will submit to the USD(I&S) for approval the DSS templates for those FOCI mitigation or negation agreements identified in subparagraph 3.d.(3) of this enclosure 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&S), provided DSS notifies the OUSD(I&S) SPOD of the deviation from the template. DSS may provide this notification through the electronic submission of an annotated copy of the modified agreement.

e. 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 in accordance with paragraph 3.d.(3)(c) of this enclosure. 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 Reference (q) 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.

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

(a) Pre-contract activities in accordance with subparagraph 3.d.(3).(c).1 of this enclosure.

(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.

(2) 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 6.b. of Enclosure 2 of this Volume, 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&S) SPOD and OUSD(AT&L), Deputy Assistant Secretary of Defense for Manufacturing and Industrial Base Policy, a monthly report of pending NID decisions that:

a. Exceed 30 calendar days from the date of the DSS written notice to the applicable GCA.

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

(b) OUSD(I&S) 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 3.c. of this enclosure 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:

a. 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&S) SPOD.

b. 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.

c. 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.

f. Government Security Committee (GSC)

(1) 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 Reference (j) 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 Reference (j) 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 a Technology Control Plan (TCP).

(2) 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 or negation agreement and related documents, contract security requirements, USG export control laws, and the NISP.

(3) In the case of an SSA, DSS will ensure that the number of outside directors exceeds the number of inside directors. 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.

(4) 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 Reference (j). 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.

g. TCPs. Under a VTA, PA, SSA, SCA, or Limited FCL, DSS will require the contractor to develop and implement a TCP as required in Reference (j). 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.

h. 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.

i. 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.

j. Annual Review and Certification

(1) Annual Meeting. DSS will meet at least annually with the GSCs of contractors 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 Facility Security Officer (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.

(2) 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.

k. Foreign Government Ownership or Control

(1) In accordance with Reference (r), 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.

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

(3) 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 (Reference (s)). The GCA will request the waiver from the USD(I&S) and provide supporting information, to include a copy of the proposed NID.

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

(5) If the USD(I&S) 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.

l. Changed Conditions

(1) DSS will require contractors to submit timely reports of changes to FOCI by DSS-designated means in accordance with Reference (j).

(2) 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&S) SPOD.

m. Limited FCL

(1) 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 a limited access authorization (LAA) for a non-U.S. citizen. Consideration of a Limited FCL includes a DSS determination that the contractor 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 subparagraphs 3.m.(3)(a) through 3.m.(3)(d) of this enclosure.

(2) 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 3.g. of this enclosure, that the contractor has and implements a TCP consistent with Reference (j).

(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.

(3) 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 the Department of Defense. 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 (Reference (t)). 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 Reference (j).

(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 subparagraph 3.d.(3) of this enclosure.

(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 6.b. of Enclosure 2 of this Volume, may sponsor a U.S. company determined to be under FOCI by DSS for a Limited FCL when the other FOCI security agreements described in subparagraph 3.d.(3) and subparagraphs 3.m.(3)(a) through 3.m.(3)(d) 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.

n. Foreign Mergers, Acquisitions, Takeovers, and CFIUS

(1) 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 part 800 of title 31, Code of Federal Regulations (Reference (u)).

(2) DoD is a member of CFIUS. DoD procedures for reviewing and monitoring transactions filled with CFIUS are provided in DoDI 2000.25 (Reference (v)).

(3) 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

(4) 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&S) SPOD 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 OUSD(AT&L) Manufacturing and Industrial Base Policy (MIBP) CFIUS Team electronically, with a copy to the OUSD(I&S) SPOD, 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&S) SPOD 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&S) SPOD 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).

(5) 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 Reference (j), DSS may recommend additional time through the OUSD(I&S) SPOD to resolve any national security issues related to FOCI mitigation.

(6) 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. 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.

(7) 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&S) SPOD.

(8) 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 3.b.(4) of this enclosure.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASA	Administrative Support Agreement
CFIUS	Committee on Foreign Investment in the United States
CI	Counterintelligence
COMSEC	communications security
CSA	cognizant security agency
DoDD	DoD directive
DoDI	DoD instruction
DoD SAPCO	DoD Special Access Program Central Office
DOE	Department of Energy
DoJ	Department of Justice
DSS	Defense Security Service
DTSA	Defense Technology Security Administration
ECP	electronic communications plan
E.O.	Executive Order
FCL	facility security clearance
FGI	foreign government information
FOCI	foreign ownership, control, or influence
FSO	Facility Security Officer
GCA	Government Contracting Activity
GSC	Government Security Committee
IA	information assurance
ISOO	Information Security Oversight Office
KMP	key management personnel
LAA	limited access authorization

MIPB	Manufacturing and Industrial Base Policy
NDA	non-disclosure agreement
NID	national interest determination
NISP	National Industrial Security Program
NSA	National Security Agency
NSA/CSS	National Security Agency Central Security Service
ODNI	Office of the Director of National Intelligence
OUSD(AT&L)	Office of the Under Secretary of Defense for Acquisition, Technology and Logistics
OUSD(I&S)	Office of the Under Secretary of Defense for Intelligence and Security
PA	proxy agreement
PCL	Personnel security clearance
PCLSA	Personnel security clearance assurance
PEO	Program Executive Office
RD	Restricted Data
SAP	Special Access Program
SCA	Security Control Agreement
SCI	sensitive compartmented information
SF	standard form
SPOD	Security Policy Oversight Division
SSA	Special Security Agreement
TCP	technology control plan
TS	TOP SECRET
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USG	United States Government

VTA voting trust agreement

PART II. DEFINITIONS

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

access. Defined in Reference (j).

affiliate. Defined in Reference (j).

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. This term and its definition are proposed for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms (Reference (w)).

carve-out. Defined in Reference (p).

classified contract. Defined in Reference (j).

classified information. Defined in Reference (j).

company. Defined in Reference (j).

components. DoD and non-DoD agencies for which DoD provides industrial security services in accordance with Reference (b).

COMSEC. Defined in Joint Publication 6-0 (Reference (x)).

contractor. Defined in Reference (j).

counterintelligence. Defined in Reference (w).

covered transaction. Defined in Reference (v).

CSA. Defined in Reference (j).

defense industrial base. Defined in Reference (w).

defense articles. Defined in Reference (j).

document. Defined in Reference (i).

DoD Components. 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 (hereinafter referred to collectively as the "DoD Components").

facility. Defined in Reference (j).

FCL. Defined in Reference (j).

FGI. Defined in Reference (i).

FOCI action plan. For purposes of this manual, 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 manual, 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 factors, imposes various security measures within an institutionalized set of company practices and procedures. Examples include board resolutions, security control agreements and special security agreements. This term and its definition are proposed for inclusion in the next edition of Reference (w).

FOCI negation agreement. For purposes of this manual, 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 VTAs and PAs. This term and its definition are proposed for inclusion in the next edition of Reference (w).

foreign interest. Defined in Reference (j).

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 Reference (j).

GCA. Defined in Reference (j).

industrial security. Defined in Reference (j).

information. Defined in Reference (i).

Limited Access Authorization (LAA). Defined in Reference (j).

NID. Defined in Reference (q).

non-DoD Components. Those USG executive branch departments and agencies identified in Reference (j) that have entered into agreements with the Secretary of Defense to act as the 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 Reference (b). This term and its definition are proposed for inclusion in the next edition of Reference (w).

personnel security clearance (PCL). Defined in Reference (j).

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. This term and its definition are proposed for inclusion in the next edition of Reference (w).

prime contract. Defined in Reference (j).

proscribed information. TS information, COMSEC information excluding controlled cryptographic items when unkeyed and utilized with unclassified keys, RD, SAP information, or SCI. This term and its definition are proposed for inclusion in the next edition of Reference (w).

RD. Defined in Reference (j).

SAP. Defined in Reference (i).

SCI. Defined in Reference (w).

security assurance. A written confirmation, requested by and exchanged between governments, that contains the following elements: verification of the 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 USG. 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 personnel security clearance assurance (PCLSA). This term and its definition are proposed for inclusion in the next edition of Reference (w).

subcontract. Defined in Reference (j).