BRIEFING PAPERS® SECOND SERIES

WEST®

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

NATIONAL SECURITY IMPLICATIONS OF FOREIGN INVESTMENT IN U.S. GOVERNMENT CONTRACTORS/EDITION II

By Joseph D. West, Judith A. Lee, Jose W. Fernandez, Annie Yan, and Sarah B. Gleich

As the economy recovers from the worldwide recession of recent years, foreign investment continues to be increasingly common in U.S. business. However, such foreign investment can present unique challenges and difficulties, as it can be subject to heightened review and scrutiny by the U.S. Government. Foreign investments in U.S. businesses that could result in control of the U.S. businesses by foreign persons are subject, voluntarily or involuntarily, to the national security review conducted by the interagency Committee on Foreign Investment in the United States (CFIUS) and, potentially, although rarely, blockage of the transaction by the President.[1] CFIUS review is authorized under § 721 of the Defense Production Act of 1950[2] (which was added to the original law by a 1988 amendment commonly known as the Exon-Florio amendment[3]), as amended by the Foreign Investment and National Security Act of 2007 (FINSA),[4] and as implemented by Executive Orders[5] and the regulations published by the U.S. Department of the Treasury.[6] Additionally, for companies conducting classified or other special access work, any significant foreign investment will be reviewed by the U.S. Government to ensure that any foreign control, ownership, or interest (FOCI) is properly mitigated to protect the U.S. Government's national security interests pursuant to the requirements of the National Industrial Security Program (NISP).

In the six years since the first edition of this BRIEFING PAPER was published in 2007,[7] significant changes have occurred both in terms of the CFIUS review and the U.S. Government's

IN BRIEF

Joseph D. West and Judith A. Lee are partners and Annie Yan and Sarah B. Gleich are associates in the Washington, D.C. office of Gibson, Dunn & Crutcher LLP. Jose W. Fernandez is a partner in the New York office of Gibson, Dunn & Crutcher LLP and, immediately prior to joining the firm, was Assistant Secretary of State for Economic, Energy and Business Affairs, serving as the Department of State's primary representative to the Committee on Foreign Investment in the United States. All practice in the Government Contracts and International Trade areas.

review of FOCI. The CFIUS review process has undergone significant reforms, including the enactment of FINSA in July 2007,[8] issuance of Executive Order 13,456 in January 2008,[9] revision of the CFIUS regulations in November 2008,[10] and publication by the U.S. Department of the Treasury of guidance on CFIUS's national security considerations in December 2008.[11] In the realm of the FOCI review, in 2014 the Defense Security Service (DSS) of the U.S. Department of Defense (DOD) issued an interim final rule adding to Title 32, "National Defense," of the *Code of Federal Regulations* a new Part 117 related to the NISP.[12] While not substantively changing the existing DSS practices, these NISP regulations implement uniform procedures for the analysis and mitigation of FOCI. Notably, the NISP regulations also codify a 2009 DSS Directive-Type Memorandum requiring extensive disclosure regarding the identify, composition, and ownership interests of foreign investors including, in the case of private equity or hedge-type fund investors, information regarding individual investors and debtholders.[13]

For parties to proposed foreign investments or transactions that may raise U.S. national security issues, the CFIUS review process essentially provides "safe harbor."[14] Nevertheless, before making a voluntary notification to CFIUS of a transaction with potential national security implications, parties to an international deal should carefully consider whether the prerequisites for CFIUS review involving questions of "control," "foreign person," and "national security concern" are met in light of the potential downside to making an otherwise unnecessary filing seeking review. As discussed below, CFIUS will frequently insist on certain "mitigation" conditions and agreements before finally approving a transaction, and these conditions could be avoided when there is clearly no transfer of control or implication of national security concerns.

Moreover, because the review of foreign acquisitions of U.S. companies necessarily involves a review of the "national security" concerns implicated by the proposed transaction, antitrust, export control, and other regulatory requirements must be coordinated with the CFIUS process. For example, parties should give careful consideration to the requirements of the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) in connection with transfer of existing export licenses and agreements under the International Traffic in Arms Regulations (ITAR),[15] as well as the DSS in connection with the protection of classified information.[16] And, as in any transaction involving a change in control, where the company being acquired is a U.S. Government contractor, the parties must address issues related to rights and responsibilities under the ongoing contracts.

In the light of complex issues raised for U.S. Government contractors by the U.S. Government's scrutiny of the national security implications of foreign investment in U.S. companies, this Briefing Paper discusses the laws and regulations governing the CFIUS review process, FOCI review under the NISP, the related economic sanctions and export control issues, and the rules governing conflicts of interest, assignments and novations, and name changes that U.S. Government contractors involved in a deal resulting in a change-in-control must address.

WEST®

BRIEFING PAPERS

Briefing Papers® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2014 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.legalsolutions.thomsonreuters.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

CFIUS Review

■ President's Authority

Unlike many countries, the United States does not routinely screen foreign direct investment but rather relies on certain targeted laws to ensure that such investments do not harm specific U.S. interests. Most prominently, in 1988, Congress passed the Exon-Florio amendment to the Omnibus Trade and Competitiveness Act of 1988, adding § 721 of the Defense Production Act of 1950.[17] The Exon-Florio amendment, as amended in 2007 by FINSA,[18] grants the President, acting through CFIUS, broad authority to review certain foreign acquisitions, mergers, takeovers, or investments that would give a foreign interest control of a company that is engaged in interstate commerce in the United States. Following the review, the President may suspend or prohibit the transaction if such control "threatens to impair the national security of the United States"[19] and that threat cannot be adequately addressed by other legislation (other than the International Emergency Economic Powers Act,[20] which gives the President authority to address any "unusual and extraordinary threat" to the national security, foreign policy, or economy of the United States after first declaring a national emergency).[21]

Significantly, the President's determinations under Exon-Florio are not subject to judicial review.[22] The first attempted substantive judicial review of the CFIUS process occurred only in 2013 and resulted from just the second time a President has exercised the statutory authority to block a transaction. There, Chinese investors involved in the attempted acquisition of the wind farms in Oregon—a transaction prohibited in September 2012 by President Obama—challenged the CFIUS mitigation order and the presidential order[23] in the U.S. District Court for the District of Columbia. The district court dismissed these claims and affirmed the President's broad discretion to block transactions or order divestment under Exon-Florio.[24]

■ CFIUS Membership

Legislation and Executive Orders assign the task of reviewing foreign investment to the CFIUS interagency group,[25] which carries out its responsibilities in the light of the open investment policy of the United States.[26] First created in 1975,[27] CFIUS' membership currently includes representatives from numerous U.S. Government departments and agencies, including the Departments of the Treasury (with the Secretary of the Treasury as the chairperson of CFIUS), Justice, Homeland Security, Commerce, Defense, State, and Energy, the Office of the U.S. Trade Representative, and the Office of Science and Technology Policy, as well as representatives from the Office of the Director of National Intelligence and the Department of Labor as non-voting, ex-officio members.[28] Representatives from the Office of Management and Budget, Council of Economic Advisors, National Security Council, National Economic Council, and Homeland Security Council also observe and, as appropriate, participate in CFIUS activities.[29] To successfully navigate the CFIUS review process, it is critical for parties to transactions to coordinate their response to the concerns of these different regulatory agencies.

Typically, each member of CFIUS delegates his or her authority to an official with experience relevant to analyzing international transactions that may threaten national security. For example, an official from the Office of the Deputy Under Secretary of Defense for Industrial Policy conducts the analysis for the DOD, and an official from the Office of Foreign Financial and Investment Issues participates for the Department of Homeland Security. Officials from the Bureau of Economic and Business Affairs, and in specific instances the Office of Defense Trade Controls conduct the analysis for the Department of State.

■ CFIUS Review Activity & Results

Every year, CFIUS submits an annual report to Congress summarizing its activities in the preceding year. According to the CFIUS annual report for calendar year 2012, from 2008 to 2012, CFIUS reviewed a total of 538 transactions, of which 114 transactions were reviewed in 2012, compared to 111 reviews in 2011 and 93 reviews in 2010.[30] Of the 114 transactions reviewed in 2012, most reviews were completed within the 30-day period, 45 transactions went through the additional 45-day investigation, and 22 transactions were withdrawn.[31] Of the 22 transactions that were withdrawn, new notices

were later filed for 12 of these transactions.[32] In 2012, CFIUS implemented measures to mitigate threats to national security in eight acquisitions of U.S. companies engaged in the software, information, mining, energy and technology industries.[33] As noted above, one transaction was blocked by President Obama in 2012, only the second time a President has prohibited a transaction in the history of CFIUS.[34]

Foreign investments in the manufacturing industry accounted for the greatest number of covered transactions (45 transactions in 2012).[35] Computer and electronic products accounted for more than 50% of all notices in the manufacturing industry.[36] Chinese investments represented the greatest number of reviews among all foreign countries in 2012 (23 transactions), followed by the United Kingdom (17 transactions) and Canada (13 transactions).[37] In 2012, CFIUS identified 111 foreign acquisitions of U.S. critical technology companies, with the largest amount of such transactions involving targets whose primary activities are in the aerospace and defense sectors (25 transactions).[38]

Although the CFIUS review process has only twice resulted in the President prohibiting a transaction,[39] this statistic could be deceptive. A number of proposed transactions have been abandoned or significantly restructured after initial CFIUS scrutiny signaled that approval was unlikely. The CFIUS process therefore not only allows a foreign purchaser to obtain comfort regarding the ultimate legality of a transaction but also to work with regulators to structure the transaction to avoid national security concerns. For transactions involving acquisition of a U.S. entity that holds security clearances or classified Government contracts, the companies typically negotiate with the DSS to ensure that appropriate mitigation is put into place to address concerns regarding FOCI. Issues related to the protection of classified information are discussed later in this Briefing Paper.

■ Covered Transactions

The CFIUS regulations set forth a nonexclusive list of transactions that are "covered transactions," as well as a list of transactions that are not subject to CFIUS review. Covered transactions include:[40]

> (a) A transaction which, irrespective of the actual arrangements for control provided for in the terms of the transaction, result or could result in control of a U.S. business by a foreign person.
>
> (b) A transaction in which a foreign person conveys its control of a U.S. business to another foreign person.
>
> (c) A transaction that results or could result in control by a foreign person of any part of an entity or of assets, if such part of an entity or assets constitutes a U.S. business.…
>
> (d) A joint venture in which the parties enter into a contractual or other similar arrangement, including an agreement on the establishment of a new entity, but only if one or more of the parties contributes a U.S. business and a foreign person could control that U.S. business by means of the joint venture.

The regulations use the term "transaction" to refer a proposed or completed merger, acquisition, or takeover.[41] The term includes:[42]

> (a) The acquisition of an ownership interest in an entity.
>
> (b) The acquisition or conversion of convertible voting instruments of an entity.
>
> (c) The acquisition of proxies from holders of a voting interest in an entity.
>
> (d) A merger or consolidation.
>
> (e) The formation of a joint venture.
>
> (f) A long-term lease under which a lessee makes substantially all business decisions concerning the operation of a leased entity, as if it were the owner.

According to the CFIUS regulations, the following types of transactions are *not* covered transactions subject to CFIUS review:[43]

> (a) a stock split or pro rata stock dividend that does not involve a change in control.
>
> (b) A transaction that results in a foreign person holding ten percent or less of the outstanding voting interest in a U.S. business (regardless of the dollar value of the interest so acquired), but only if the transaction is solely for the purpose of passive investment.
>
> (c) An acquisition of any part of an entity or of assets, if such part of an entity or assets do not constitute a U.S. business.…
>
> (d) An acquisition of securities by a person acting as a securities underwriter, in the ordinary course of business and in the process of underwriting.

> (e) An acquisition pursuant to a condition in a contract of insurance relating to fidelity, surety, or casualty obligations if the contract was made by an insurer in the ordinary course of business.

In addition, ordinary lending transactions are generally not covered transactions.[44]

■ Foreign Control

CFIUS review covers a broad range of acquisitions, mergers, and takeovers, *i.e.*, any transaction that could result in foreign "control" of entities engaged in interstate commerce in the United States.[45] The definition of "control" is functional and broad and is intended to be applied on a case-by-case basis.[46] "Control" is defined to mean "the power, direct or indirect, whether or not exercised, through the ownership of a majority or a dominant minority of the total outstanding voting interest in an entity, board representation, proxy voting, a special share, contractual arrangements, formal or informal arrangements to act in concert, or other means, to determine, direct, or decide important matters affecting an entity."[47] The CFIUS regulations also list 10 exemplary factors that may be considered important matters affecting an entity, including the power to sell the entity or transfer its assets, to dissolve the U.S. entity, to approve major expenditures, to close or relocate any of its facilities, to terminate its contracts, and to appoint or dismiss officers.[48]

The CFIUS regulations do not define what level of ownership triggers review. The determination of who has control of an entity does not, therefore, turn merely on the percentage of ownership, but also on who has potential decisionmaking power. The amount of equity interest held by a foreign person and the right to elect board members to a U.S. business are important, but not determinative, factors in finding control. If a foreign person acquires 10% or less of the outstanding voting interest in a U.S. company solely for passive investment purposes, the transaction will not trigger CFIUS review.[49]

■ Minority Shareholder Rights

The CFIUS regulations appear to envision that a foreign minority shareholder could, under some circumstances, exercise control over a U.S. company for purposes of CFIUS review if it could affect the material corporate decisions of the company.[50] Clarifying examples of transactions and structures are provided in the regulations.[51] Certain minority shareholder protection measures, however, such as the power to prevent the voluntary filing of bankruptcy or liquidation and the power to prevent the change of existing legal rights or preferences of a particular class of stock held by minority investors, do not confer control. CFIUS will consider whether a minority shareholder right confers control on a case-by-case basis. The regulations make it clear that the following minority shareholder protections do not in themselves confer control:[52]

> (1) The power to prevent the sale or pledge of all or substantially all of the assets of an entity or a voluntary filing for bankruptcy or liquidation;
>
> (2) The power to prevent an entity from entering into contracts with majority investors or their affiliates;
>
> (3) The power to prevent an entity from guaranteeing the obligations of majority investors or their affiliates;
>
> (4) The power to purchase an additional interest in an entity to prevent the dilution of an investor's *pro rata* interest in that entity in the event that the entity issues additional instruments conveying interests in the entity;
>
> (5) The power to prevent the change of existing legal rights or preferences of the particular class of stock held by minority investors, as provided in the relevant corporate documents governing such shares; and
>
> (6) The power to prevent the amendment of the Articles of Incorporation, constituent agreement, or other organizational documents of an entity with respect to the matters described in paragraphs (1) through (5) above.

Although the regulations do not provide examples of minority shareholders' rights that do convey "control" under CFIUS, several important protections generally sought by minority investors, such as the power to prevent the company from adopting or modifying a business plan or entering into certain agreements, may result in a determination of control.[53] Thus a shareholder negotiating supermajority protection rights may find that the more successful its negotiations, the more likely it is to come under the purview of CFIUS.

■ U.S. Business; Foreign Person

The definition of a "covered transaction" focuses on "U.S. businesses" rather than "U.S. persons."[54] The terms "U.S. business" and "foreign person" are defined broadly to bring some foreign–foreign and some U.S.–U.S. transactions within its scope. The term "U.S. business" means "any entity, irrespective of the nationality of the persons that control it, engaged in interstate commerce in the United States, but only to the extent of its activities in interstate commerce."[55] The controlling investments in a business not organized as a legal entity (e.g., assets sale or sale of a business unit) may still be subject to CFIUS review.[56] A "foreign person" is any "foreign national, foreign government or foreign entity" or any "entity over which control is exercised or exercisable by a foreign national, foreign government, or foreign entity."[57]

A "foreign entity" is an entity "organized under the laws of a foreign state if either its principal place of business is outside the United States or its equity securities are primarily traded on one or more foreign exchanges."[58] However, if U.S. nationals own more than 50% of the entity, it will not be considered a foreign entity.[59] Therefore, a U.S. subsidiary of a foreign company can be both a "U.S. business" and a "foreign person." The determination of a "U.S. business" is not based on the nationality of the owners or the place of incorporation of an entity, but rather on whether the entity is engaged in interstate commerce in the United States.[60] The determination of a "foreign person," on the other hand, is based on whether an individual or entity is controlled by a foreign interest, not on where it does business. Therefore, both the acquisition of a foreign company's U.S. subsidiary by another foreign company and the acquisition of a U.S. company by the U.S. subsidiary of a foreign company may be subject to the CFIUS review.

■ National Security

Determining whether a transaction threatens to impair U.S. national security also requires CFIUS to weigh a variety of facts and circumstances. Neither the CFIUS laws nor the implementing regulations define "national security," resulting in case-by-case determinations. The President and CFIUS may consider the following factors in deciding whether U.S. national security will be impaired by a transaction:[61]

> (1) domestic production needed for projected national defense requirements,
>
> (2) the capability and capacity of domestic industries to meet national defense requirements, including the availability of human resources, products, technology, materials and other supplies and services,
>
> (3) the control of domestic industries and commercial activity by foreign citizens as it affects the capability and capacity of the United States to meet the requirements of national security,
>
> (4) the potential effects of the proposed or pending transaction on sales of military goods, equipment, or technology to [particular countries deemed to pose a threat to the United States]…;
>
> (5) the potential effects of the proposed or pending transaction on United States international technological leadership in areas affecting United States national security;
>
> (6) the potential national security-related effects on United States critical infrastructure, including major energy assets;
>
> (7) the potential national security-related effects on United States critical technologies;
>
> (8) whether the covered transaction is a foreign government-controlled transaction…;
>
> (9) as appropriate…a review of the current assessment of—
>
> (A) the adherence of the subject country to nonproliferation control regimes, including treaties and multilateral supply guidelines…;
>
> (B) the relationship of such country with the United States, specifically on its record on cooperating in counter-terrorism efforts…; and
>
> (C) the potential for transshipment or diversion of technologies with military applications, including an analysis of national export control laws and regulations;
>
> (10) the long-term projection of United States requirements for sources of energy and other critical resources and material; and
>
> (11) such other factors as the President or CFIUS may determine to be appropriate, generally or in connection with a specific review or investigation.

Whether a proposed transaction poses a national security risk is the most difficult—and often controversial—determination CFIUS can

make. Beginning with the deliberations that culminated in the enactment of the Exon-Florio amendment, lawmakers and policy analysts have debated whether "national security" should be broadly construed to encompass "economic security" and whether CFIUS should be concerned with foreign acquisitions that affect the competitiveness of particular U.S. industries, and there have been efforts to advance such arguments during the review of various transactions. Other transactions raise the question whether a foreign purchaser's elimination of U.S. jobs is an appropriate consideration in a CFIUS review. However, issues of national competitiveness, as opposed to strict national security concerns, have not been deemed relevant to the CFIUS analysis. CFIUS investigations might also be concerned with the protection of classified information, significant reductions in competition for critical defense contracts, potential transfers of technology to foreign parents, partners, or customers, and the location of the targeted business close to defense facilities.

The factors in paragraphs (6) to (10) above were added by FINSA,[62] which provides for special review of transactions involving "critical infrastructure," including "major energy assets"[63] and transactions involving "critical technologies." "Critical infrastructure" is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security."[64] This would include, for example, in addition to energy assets, communications and transportation systems and facilities. "Critical technologies" are defined in the implementing regulations as (a) defense articles or defense services covered by the United States Munitions List as set forth in the ITAR,[65] (b) those items specified on the Commerce Control List set forth in Supplement No. 1 to Part 774 of the Export Administration Regulations (EAR)[66] that are controlled pursuant to multilateral regimes (*i.e.*, for reasons of national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology), as well as those that are controlled for reasons of regional stability or surreptitious listening, (c) specially designed and prepared nuclear equipment, parts and components, materials, software, and technology specified in the Assistance to Foreign Atomic Energy Activities regulations[67] and nuclear facilities, equipment, and material specified in the Export and Import of Nuclear Equipment and Material regulations,[68] and (d) select agents and toxins specified in the Select Agents and Toxins regulations.[69] The addition of these factors by FINSA widens CFIUS' discretion to intervene in a transaction, giving it authority to identify strategically important industries and granting specific encouragement to investigate transactions involving internet-related industries.

FINSA heightens CFIUS scrutiny of transactions involving foreign state-owned entities. A full CFIUS investigation is required with respect to any "foreign government-controlled transaction,"[70] meaning a covered transaction that could result in control of a U.S. business by a foreign government or a person owned or controlled by or acting on behalf of a foreign government.[71] When a foreign government-controlled entity is involved, FINSA requires the consideration of factors not necessarily related to the transaction at hand, such as a country's compliance with U.S. and multilateral counter-terrorism, nonproliferation, and export control regimes.[72] In addition, a full CFIUS investigation is also mandatory with respect to certain transactions involving critical infrastructure.[73]

In December 2008, the U.S. Department of the Treasury published guidance with respect to CFIUS reviews.[74] The Treasury guidance describes the purpose and nature of the CFIUS process, how CFIUS analyzes whether a transaction poses national security risks, national security factors identified by FINSA, and the types of transactions that CFIUS has reviewed that have presented national security considerations.

■ CFIUS Review Process & Timing

For transactions subject to CFIUS review, the review process is usually initiated once the parties have voluntarily submitted notice of the transaction. Any party to the transaction may—but is not required to—request a review of the transaction's national security implications.[75] In other words, a CFIUS notice is nominally made by the parties to a transaction as a *voluntary* undertaking. However, the voluntary character of the filing is

somewhat deceptive. In fact, if CFIUS believes a transaction is a covered transaction that may raise national security concerns, CFIUS may request the parties to a covered transaction to file a notice.[76] In addition, any member agency of CFIUS may initiate a review by submitting an agency notice to CFIUS.[77] Such involuntary reviews are rare and disfavored, and, when they occur, may not put the parties in the best light with CFIUS. In a case of a transaction that is likely to present national security concerns, but for which the parties have not notified CFIUS, CFIUS is most likely to inquire informally and suggest that the parties file voluntarily, eliminating the need to initiate an involuntary review.

Parties to the transactions are encouraged, but not required, to engage in pre-notice consultations with CFIUS prior to formally notifying CFIUS of a transaction.[78] A pre-notice consultation should take place at least five business days prior to a formal filing.[79] Once a formal voluntary notice is filed, CFIUS has 30 days to decide whether to conduct a full investigation.[80] If CFIUS decides that no investigation is needed, the review process is concluded.[81] If CFIUS decides that a full investigation is warranted, it must complete its work and submit a report on its findings to the President within 45 days.[82] The President then has 15 days to announce his intended course of action, which may include taking no action, prohibiting a proposed transaction, or, in the event that the transaction has been consummated, ordering a divestiture.[83] As discussed above, a full investigation is mandatory with respect to a foreign government-controlled transaction and is more likely in complex transactions and transactions involving critical infrastructure.[84]

■ Contents Of Notice

If parties to a transaction decide to file a voluntary notice with CFIUS, they must submit extensive information in the filing.[85] A voluntary notice of the transaction may be submitted by sending one paper copy and one electronic copy of the required information by email to the Staff Chairperson of CFIUS.[86]

The filing burden is greater in transactions involving significant sales to U.S. defense and homeland security agencies.[87] For defense transactions, parties must report whether the Government contracts implicated in the transaction are for sole-source or single qualified source products or are priority-rated contracts,[88] and parties must provide information for contracts in effect within the past three years with a U.S. Government agency with national defense, homeland security or other national security responsibilities.[89] Parties must also address whether a cybersecurity plan exists with respect to protecting the U.S. business, provide the U.S. market share for product and service categories of the U.S. business and the methodology to determine the market share, provide information on products that are supplied to third parties and rebranded, and provide a curriculum vitae of the board members and senior officers of the acquiring foreign person, including their military service.[90]

After the initial filing of the voluntary notice, parties to a transaction must respond to additional information requests from CFIUS within three business days, unless an extension request is granted.[91]

■ CFIUS Review As "Safe Harbor"

Generally, no CFIUS notice, review, or investigation can occur more than three years after the date of the transaction.[92] However, the Chairperson of CFIUS may, in consultation with other members, request an investigation after the three years has passed.[93] Thus, transactions for which CFIUS does not receive notice potentially remain forever open to scrutiny. On the other hand, once a transaction clears CFIUS review or the President has decided to allow it, the transaction may not be reinvestigated unless the initial review was based on materially incorrect or incomplete information, or a party to the transaction has "intentionally materially" breached a mitigation agreement or condition imposed by CFIUS.[94] Consequently, it is often in the parties' interest to notify CFIUS of a transaction involving a foreign entity early in the process to avoid lingering uncertainty. The CFIUS process is confidential, and CFIUS does not publish its decisions.[95] Failure to file and obtain a favorable determination from CFIUS in advance could result in transaction delays,

disruptions, and possible forced divestment after the closing of the transaction.[96]

■ Civil Penalties

The implementing regulations authorize CFIUS to impose a civil fine up to $250,000 per violation against a person who, internationally or through gross negligence, submits a material misstatement or omission in a notice or makes a false certification to CFIUS[97] as well as a civil fine up to the greater of $250,000 or the value of the transaction against a person who, intentionally or through gross negligence, violates a material provision of a mitigation agreement.[98] In addition, CFIUS may also negotiate for liquidated damages provisions in mitigation agreements.[99]

■ Risk Mitigation

During a review, CFIUS may insist that the parties implement structural safeguards, such as a firewall concealing certain matters from foreign management, in cases in which foreign persons purchase U.S. companies that do national security work. Mitigation measures were used for eight transactions in 2012 covering businesses in software, information, mining, energy, and technology industries.[100]

As discussed in more detail below, the industrial security regulations, which are published by the Under Secretary of Defense for Intelligence and administered by the DSS, set forth several measures that defense companies under foreign ownership or control may undertake to mitigate the risks posed by foreign ownership and obtain a security clearance or assume the clearance of a U.S. company that already has a clearance. These measures, which are described in the National Industrial Security Program Operating Manual (NISPOM), include proxy arrangements, which enable U.S. managers to exclude foreign owners from certain aspects of the company's classified business, and other special security arrangements intended to segregate foreign owners from sensitive operations.[101] These regulations often play an important role in guiding a CFIUS review process that involves a U.S. company with classified contracts. The interrelationship between increased CFIUS scrutiny and heightened security concerns is evident in the DSS's extensive information disclosure and mitigation requirements for foreign ownership situations.

■ Impact Of FINSA

The increased scrutiny of foreign investment under FINSA challenges Government contractors' abilities to raise funds from foreign investors and to seek business opportunities through mergers and acquisitions. It can also work at cross-purposes with respect to the Obama Administration's efforts to increase foreign direct investment into the United States, more recently with the "Select USA" initiative.[102] CFIUS' broader mandate and scope of review will mean that more transactions are reviewed. This broader review has focused on technology and infrastructure sectors, which affects contractors in defense, energy, and high-technology sectors.

FINSA also creates greater possible transaction delays and increases financial risks accordingly. As noted, FINSA mandates the extension of national security reviews beyond the 30-day clearance period to the supplemental 45-day investigation phase in some cases. It requires that CFIUS investigate acquisitions involving sensitive critical infrastructure, unless major relevant Government agencies approve the deal at the highest levels.[103] This mandated extension of the review period effectively shifts the burden of proof to the transaction parties in some cases, who must now convince political appointees that an extended review is unnecessary.

The level of required congressional oversight arguably exposes deals to the unpredictable winds of politics and public sentiment. FINSA requires CFIUS to brief Congress on its reviews and to provide annual reports.[104] CFIUS must give Congress notice of each review it makes, its actions, and its conclusions.[105] This transaction-specific political analysis could potentially open the door to myriad potential political obstacles. For example, an organized or concentrated political interest could commandeer the review process to seek a competitive advantage against a foreign investor or to exact a political penalty against its home country.

National Industrial Security Program

One of the primary factors that CFIUS will review, and that in some cases may drive its determination as to the acceptability of the transaction, is whether the target company holds a security clearance, and, if so, the extent of the target's classified contracts. For this reason, no CFIUS notification is complete without a discussion as to how the Government's interests in protecting classified and other access-restricted information will be protected.

Notably, even if a determination is made that a voluntary CFIUS notification is not required, a cleared company with a reportable increase in foreign ownership or control must still notify the Government of this change.[106] In considering whether or not to make a CFIUS notification, a company should consider that, under the NISP regulations, the DSS is required to inform CFIUS if it is notified of a transaction with respect to which the parties have not previously filed a notice with CFIUS.[107]

■ Government Contractor Clearance Requirements

The NISP was established by Executive Order 12,829 to protect classified information "that is released to contractors, licensees, and grantees of the United States Government."[108] Four Cognizant Security Agencies (CSAs) of the Executive Branch have been authorized to establish industrial security programs: the DOD, the U.S. Department of Energy (DOE), the Office of the Director of National Intelligence, and the U.S. Nuclear Regulatory Commission (NRC).[109] The Secretary of Defense acts as the Executive Agent for the NISP and has final responsibility, through the DSS, for issuing and maintaining the NISPOM, which prescribes "the requirements, restrictions, and other safeguards to prevent unauthorized disclosure of classified information."[110] The DSS provides industrial security services for the DOD, the NRC, and 26 other agencies.[111] Historically, the requirements for contractors and their employees to obtain and maintain facility and personnel security clearances in order to gain access to classified information in their performance of a U.S. Government contract with a covered agency were laid out in the NISPOM and various DSS directives, industrial security letters, and guidance. In 2014, the DOD added Part 117, "National Industrial Security Program," to Title 32 of the *Code of Federal Regulations*.[112] Focused exclusively on FOCI,[113] the NISP regulations provide baseline requirements for the U.S. Government's evaluation of a foreign owner's rights and determination as to whether those rights can be mitigated to effectively protect classified information and preclude its unauthorized disclosure.[114] While not substantively changing the existing DSS policy regarding FOCI analysis and mitigation, the NISP regulations do establish standard procedures including set timelines for certain events, most notably the processing of a National Interest Determination (NID).[115]

In addition to the NISPOM, which serves as "the national standard to establish the baseline requirements for contractor [facility security clearances]," the DOE maintains its own Safeguards and Security Program (S&S Program) providing supplemental requirements for the protection of DOE-specific assets, Restricted Data, Special Nuclear Material, and other security activities not covered by the NISPOM.[116]

■ Facility Security Clearance

The NISPOM and the S&S Program require a company to obtain a facility security clearance before it is eligible to access classified information under a U.S. Government contract. The NISPOM defines a facility security clearance as an "administrative determination that, from a security viewpoint, a company is eligible for access to classified information of a certain category (and all lower categories)."[117]

To be eligible for a facility security clearance, a contractor must (a) need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement, (b) be organized and located in the United States,[118] (c) have a reputation for integrity and lawful conduct in its business dealings, and (d) not be under foreign ownership, control, or influence.[119] If a company is owned, controlled, or influenced by a foreign interest, it will be

unable to obtain or maintain a facility security clearance unless certain mitigation methods are implemented to negate risks to U.S. security, as discussed below.[120] Without a facility security clearance, a company will be unable to perform work under classified U.S. Government contracts or to obtain classified information.[121]

■ Personnel Security Clearance

A company's employees and consultants must each obtain a personnel security clearance if they will require access to classified information in their performance of work under a U.S. Government contract.[122] The NISPOM defines a personnel security clearance as an "administrative determination that an individual is eligible, from a security point of view, for access to classified information of the same or lower category as the level of the personnel clearance being granted."[123] Employees' personnel security clearances are processed and held by their employer, so such a clearance may not be maintained absent a facility security clearance.[124]

Only employees who are U.S. citizens are eligible for personnel security clearances, and companies must make certain that "[e]very effort shall be made to ensure that non-U.S. citizens are not employed in duties that may require access to classified information."[125] In rare circumstances, however, the DSS may grant a non-U.S. citizen a Limited Access Authorization (LAA) if the individual possesses a "unique or unusual skill or expertise that is urgently needed" to support a Government contract that requires "access to specified classified information and a cleared or clearable U.S. citizen is not readily available."[126] It should be noted that an LAA is not valid for access to top secret information, restricted data, formerly restricted data, information that has not been determined releasable to the country of which the individual is a citizen, communications security information, intelligence information, North Atlantic Treaty Organization information, information for which foreign disclosure has been prohibited in whole or in part, information provided to the U.S. Government in confidence by a third-party government, or classified information furnished by a third-party government.[127]

■ Foreign Interest

If a company has a facility security clearance, that clearance may be revoked or adjusted if a foreign interest acquires an interest in or control of that company.[128] The NISPOM defines a "foreign interest" as any "foreign government, agency of a foreign government, or representative of a foreign government; any form of business enterprise or legal entity organized, chartered or incorporated under the laws of any country other than the United States or its territories, and any person who is not a citizen or national of the United States."[129]

■ FOCI Factors

A U.S. company is considered to be under FOCI: [130]

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

In determining whether a company is under FOCI, the Government will consider the source, nature, and extent of FOCI, including whether foreign interests hold a majority or substantial minority position in the company, taking into consideration the immediate, intermediate, and ultimate parent companies.[131] A minority position is deemed substantial if it consists of greater than 5% of the ownership interests or greater than 10% of the voting interest.[132] Additionally, the Government will consider factors related to the cleared company, the foreign interest, and the government of the foreign interest:

(1) the record of economic and government espionage against U.S. targets;

(2) the record of enforcement and/or engagement in unauthorized technology transfer;

(3) the type and sensitivity of the information that will be accessed;

(4) the record of compliance with pertinent U.S. laws, regulations, and contracts;

(5) the nature of any pertinent bilateral and multilateral security and information exchange agreements;

(6) whether there is ownership or control, in whole or in part, by a foreign government; and

(7) for DOE, whether the government of the foreign interest has industrial security and export control regimes in place that are comparable to those of the United States.[133]

■ Notification To The Government Of A Change In FOCI

It is important that the parties notify the appropriate Government officials in advance of any foreign acquisition in order that the U.S. company, the foreign acquirer or investor, and the U.S. Government might discuss potential FOCI mitigation methods. Indeed, a company is required to notify the CSA when it enters into negotiations for a proposed merger, acquisition, takeover, or investment by a foreign interest.[134] Generally, reportable material changes related to foreign ownership are those changes that would introduce a new threshold or factor under the FOCI analysis that did not previously exist, for instance an increase in beneficial ownership by a foreign interest of 5% or greater.[135] A U.S. company determined to be under FOCI is ineligible for an FCL unless the DSS determines security measures to mitigate the FOCI are in place.[136] Thus, failure to notify the DSS and provide an appropriate FOCI action plan can lead to suspension or revocation of a company's FCL.

As part of the CSA's determination as to whether FOCI exists, the company is required to submit information regarding (a) the type of transaction under negotiation (stock purchase, asset purchase, etc.), (b) the identity of the potential foreign interest investor, (c) a plan to negate the FOCI, and (d) copies of the loan, purchase, and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, and reports filed with other U.S. Government agencies.[137]

Notably, the extensive information required by the Government to evaluate FOCI can present an obstacle to private equity or hedge-type fund investors not accustomed to inquiring into, and, moreover, disclosing, information regarding the identify, composition, and ownership interests of its individual investors and debtholders. In circumstances in which multiple investment vehicles obtain interest in a company, it may be difficult or impossible to obtain this information for all individual investors with an interest in the vehicles. Nonetheless, both the DSS and the DOE specifically state that companies may not be eligible for a facility security clearance in cases where the identification of a foreign owner cannot be adequately ascertained.[138] Accordingly, at the outset of any transaction involving a fund including some foreign investment, consideration must be paid to (1) whether investors will be willing and able to identify and disclose the percentage of foreign ownership interest, and (2) if not, whether the company's value is substantially diminished by loss of the ability to do classified work.

■ Remedies & Mitigation Of Foreign Control

If it is determined that, upon a foreign interest's acquisition of a company, the company will be under FOCI, certain mitigation measures must be implemented to mitigate the risks associated with FOCI and, thus, to allow the company to maintain its security clearance. Furthermore, mitigation of FOCI risks can be critical to a company's ability to obtain CFIUS approval of its transaction with the foreign acquirer or investor. As a result, a company should raise potential FOCI mitigation methods with the CSA early on and obtain the CSA's approval of the selected method before CFIUS review. Such advance approval from the CSA should assist in expediting the CFIUS review process.

The NISP regulations, NISPOM, and S&S Program recognize the following mitigation methods that may be employed to negate the effect of FOCI:

(1) *Board Resolution Excluding Foreign Interest From Access To or Influence Over Classified or Export-Controlled Information*—A board resolution may be used when the foreign interest does not own voting stock sufficient to elect a representative to the company's governing board.[139] For example,

if a foreign interest owns 10% of the company's voting stock and that 10% stock ownership does not allow the foreign interest to appoint a representative to the company's board of directors, a board resolution may be adequate. This resolution effectively excludes foreign shareholders or creditors from any access to or influence over the performance of classified work. The company's governing board is required to (a) identify all foreign shareholders and the type and number of foreign-owned shares, (b) identify all foreign creditors and the corresponding details of the debt, including the type of debt, the identity of associated administrative and collateral agents and trustees, the maturity date, the outstanding principal amount of debt held by the foreign interest, and the ratio of that amount to the equity of the company, (c) acknowledge the company's obligation to comply with all industrial security program and export control requirements, and (d) certify that the foreign owner does not require, shall not have, and can be precluded from unauthorized access to classified information or influence over performance on classified contracts.[140] The board must annually certify the continued effectiveness of this resolution and distribute the resolution to the members of its governing board and key management personnel.[141]

(2) *Security Control Agreement and Special Security Agreement*—The Security Control Agreement (SCA) and the Special Security Agreement (SSA) are mitigation arrangements that preserve the foreign interest's right to be represented on the company's board through inside directors with a direct voice in the business management of the company while denying unauthorized access to classified information by these inside directors.[142] These arrangements impose substantial industrial security and export control measures within an institutionalized set of corporate practices and procedures.[143] Specifically, they provide for the establishment of a Government Security Committee (GSC) to oversee classified and export control matters and further require the active involvement of senior management and cleared, U.S. citizen outside directors in security matters.[144]

An SCA is used when the company is not effectively owned or controlled by a foreign interest, but the foreign interest is entitled to representation on the company's governing board.[145] For example, if a foreign interest owns 25% of the company's voting stock and that 25% ownership allows the foreign interest to appoint a representative to the company's governing board, an SCA may be adequate. Under an SCA, the governing board must include at least one cleared U.S. citizen outside director, approved by the CSA, who must be "completely disinterested…with no prior involvement with the company, the entities with which it is affiliated, or the foreign owner," and the chair of the board and key management personnel must be U.S. citizens who have, or are eligible to possess, a personnel security clearance.[146] Notably, an SCA has no limitations on the type of information a company may access under its FCL.[147]

An SSA is utilized when a company is determined to be effectively owned or controlled by a foreign interest.[148] Under an SSA, the company's board must consist of a minimum of (a) three cleared U.S. citizen outside directors who must be "completely disinterested individuals with no prior involvement with the company, the entities with which it is affiliated, or the foreign owner," (b) one inside director representing the parent corporation, and (c) one or more cleared officers of the company, although the combined total of inside directors must not exceed the combined total of outside directors and officer/directors.[149] As under the SCA, the chair of the board and key management personnel must be U.S. citizens who have, or are eligible to possess, a personnel security clearance, and, in addition, the chair may not be an inside director.[150] Under an SSA, in order for a company to access proscribed information,[151] the Government contracting agency requiring access to this information may be required to complete a NID to determine that the release of this proscribed information will not harm the U.S. national security requirements.[152] Notably, so long as there is no indication that the NID will be denied, the CSA can move forward with implementation of a FOCI action plan pending completion of the NID process.[153]

Under both the SCA and SSA arrangements, as well as the Proxy and Voting Trust agreements discussed below, the company must annually sub-

mit an implementation and compliance report detailing (1) the manner in which the company is carrying out its obligations under the agreement, (2) changes or impending changes to security procedures and the rationale for such changes, (3) acts of noncompliance and steps taken to prevent future recurrence, (4) changes or impending changes to key management personnel or key board members, (5) any changes or impending changes to the organizational structure or ownership of the company, or (6) any other issues that could bear on the effectiveness of the agreement.[154]

(3) *Proxy Agreement and Voting Trust Agreement*—A Proxy Agreement (PA) or a Voting Trust Agreement (VTA) is used when a company is owned or controlled by a foreign interest and the DSS determines that more restrictive measures are required to mitigate that ownership or control.[155] In these arrangements, the foreign owner relinquishes most of their ownership rights to cleared U.S. citizens approved by the CSA.[156] Specifically, under a PA, the foreign owner's voting rights are conveyed to proxy holders, and, under a VTA, the foreign owner transfers legal title in the company to trustees.[157] As these arrangements insulate the foreign owners from any control over the management of the company, neither arrangement imposes restrictions on the company's eligibility to have access to classified information or to compete for classified contracts.[158] Notably, the DSS explicitly reserves the discretion to deny the adequacy of either arrangement, meaning that, in such circumstances, there would be no available means for a company to mitigate FOCI and retain its security clearance.[159]

Establishment of a PA or a VTA involves the selection of proxy holders or trustees who serve as directors of the cleared company's board.[160] Notably, these proxy holders or trustees must be "completely disinterested individuals with no prior involvement with the company, the entities with which it is affiliated, or the foreign owner."[161] The proxy holders or trustees exercise all of the prerogatives of ownership with complete freedom to act independently from the foreign stockholders, except that proxy holders or trustees must obtain approval from the foreign shareholder regarding (a) the sale or disposal of the corporation's assets or a substantial part, (b) pledges, mortgages or other encumbrances on the capital stock, assets, or ownership interests, (c) corporate mergers, consolidations, or reorganizations, (d) the dissolution of the corporation, and (e) a filing of a bankruptcy petition.[162]

The Proxy Holder or Trustees assume full responsibility for the voting stock and for exercising all management prerogatives, except in the aforementioned instances. Under both arrangements, the DSS requires the company to annually submit the implementation and compliance report as discussed in regards to SCAs and SSAs above.[163]

(4) *Limited Facility Clearance*—A foreign-owned company may be eligible for a limited facility security clearance without any required mitigation plan if (a) there is an Industrial Security Agreement with the foreign government of the country from which the foreign ownership is derived, and (b) release of classified information is in conformity with the U.S. National Disclosure Policy.[164] The U.S. Government negotiates Industrial Security Agreements as an Annex to the General Security Agreement that is negotiated with a foreign country.[165] The General Security Agreement is an agreement that requires "each government [to] provide to the classified information provided by the other substantially the same degree of protection as the releasing government."[166] Therefore, if the foreign country has an Industrial Security Agreement with the United States, a limited facility clearance may be issued if the CSA determines that the U.S. National Disclosure Policy would allow such a release of classified information.[167]

■ Additional Mitigation Measures

A company operating under one of the aforementioned FOCI mitigation instruments may further be required to develop additional procedures to ensure that FOCI is effectively mitigated. These procedures include:

(a) *Affiliated Operations Plan*—Unless prior approval is obtained from the CSA and the company GSC, a FOCI-mitigated company may not share with its affiliates certain business functions, including affiliated services, shared third-party

services, shared persons, or cooperative commercial arrangements.[168] Where the CSA authorizes such affiliated services, the company will be required to develop an Affiliated Operations Plan that provides a detailed description of the shared operations, associated risk and applicable mitigation procedures to address such risk, and procedures to review and document plan compliance.[169]

(b) *Facilities Location Plan*—Unless prior approval is obtained from the CSA, a FOCI-mitigated company may not be located proximate to an affiliate, such as in the same building, campus, or adjoining building, where such "collocation" may reasonably inhibit the company's ability to comply with its FOCI agreement.[170] Where collocation is approved, the company GSC must establish a Facilities Location Plan providing details regarding the justification for the collocation, the relationship between the collocated affiliates, floor plans and building diagrams detailing the physical collocation, and any compliance or additional mitigation measures implemented to address increased risk to industrial security related to this collocation.[171]

(c) *Technology Control Plan*—Companies mitigating their FOCI with an SCA, SSA, PA, or VT, must implement a Technology Control Plan prescribing all technology control security measures deemed necessary to foreclose the possibility of unauthorized access to classified or export-controlled information by non-U.S. citizen employees or visitors, or company affiliates, including foreign shareholders or affiliates.[172]

(d) *Electronic Communications Plan*—For companies mitigating their FOCI with an SCA, SSA, PA, or VT, the GSC is required to establish an Electronic Communications Plan providing extensive written policies and procedures to assure there is no unauthorized disclosure of classified or export controlled information in electronic communications between the company and its subsidiaries or affiliates.[173]

(e) *Visitation Plan*—Companies mitigating their FOCI with an SCA, SSA, PA, or VT, must establish written procedures for visitation between the FOCI-mitigated company and its affiliates. Under these plans, certain restrictions are imposed including the requirement that notice of all visits be provided, in advance, to the GSC for review and written approval.[174]

Related Economic Sanctions & Export Control Issues

In addition to CFIUS review, other laws and regulations enforced by the U.S. Government seek to protect disclosure and transfer of sensitive information and technology to countries, entities, and individuals that are hostile to U.S. interests. These laws and regulations set forth principles that may inform CFIUS' review of a particular transaction, as described below.

■ Economic Sanctions

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) maintains and enforces economic sanctions against a number of countries, including Cuba, Iran, North Korea, Sudan, and Syria, as well as particular individuals and entities (termed "specially designated nationals" or "SDNs").[175] The sanctions enforced by OFAC apply to U.S. persons and entities, including (1) U.S. citizens and U.S. permanent residents, wherever located, (2) all persons physically present in the United States, regardless of nationality or residency status, and (3) businesses organized under U.S. laws, including foreign branches and other controlled offices and affiliates not separately organized under foreign laws. U.S. sanctions enforced against Iran,[176] Cuba,[177] and North Korea[178] also apply to foreign subsidiaries of U.S. companies and other non-U.S. companies that are owned or controlled by U.S. persons. The sanctions generally prohibit all or nearly all transactions between U.S. persons and (a) the government (including government-owned or controlled entities) of a sanctioned country and (b) individuals and entities in those countries. Moreover, U.S. persons may not enter into transactions with any individual or entity designated by OFAC as an SDN. In addition, the sanctions prohibit "evasion" of the sanctions and "facilitation" by U.S. persons of transactions that would otherwise occur outside of U.S. jurisdiction. "Evasion" of U.S. sanctions laws may occur when a U.S.

person refers or steers a prohibited transaction or investment to another individual or entity to whom the transaction is otherwise not prohibited.[179] The related concept of "facilitation," which OFAC interprets broadly, occurs when a U.S. person provides a medium through which non-U.S. persons can complete a transaction that would be prohibited to the U.S. person or approves, supports, or assists non-U.S. persons with entering into or implementing a transaction that would be prohibited to the U.S. person.[180]

Accordingly, CFIUS is likely to review transactions that may result in the release of information or transfer of technology to a sanctioned government, entity, or individual only with a high degree of skepticism. Indeed, the regulations prescribing the contents of a voluntary notice to CFIUS specifically request that the parties to a transaction detail the nationality of the foreign person making the acquisition, the nationality of the acquirer's parents and affiliates, and the nationality of any persons or interests that will control the U.S. company being acquired post-transaction.[181] Additionally, the company being acquired may wish to conduct due diligence regarding the foreign acquirer before consummating the transaction to ensure that it is not violating the sanctions by transacting with that foreign person.[182]

■ Export Controls

(1) *Dual-Use Export Controls Enforced by the U.S. Department of Commerce*—The U.S. Department of Commerce's Bureau of Industry and Security (BIS) enforces the export controls set forth in the EAR.[183] These export controls regulate the unlicensed transfer and retransfer of U.S.-origin goods and technology by any individual or entity, regardless of nationality or residency status, to (a) particular countries, (b) particular individuals and entities, (c) any individuals or entities engaged in particular activities (prohibited end-uses), and (d) foreign nationals who are not permanent U.S. residents, even if employed in the United States or abroad by a U.S. person ("deemed exports"). The EAR restrict the transfer of dual-use goods, technology, and services that have potential military or strategic applications. Individuals and entities that wish to export items subject to the EAR must obtain an export license from BIS before transferring any controlled items to a prohibited destination.

Because of the potential national security implications associated with transferring items or technology that may have military applications to foreign countries, CFIUS carefully reviews foreign acquisitions of U.S. companies that lawfully export controlled items and technology pursuant to an export license. The regulation that prescribes the contents of a voluntary notice to CFIUS specifically requests information regarding any products manufactured by the U.S. person being acquired that have potential military applications.[184] Moreover, the same regulation requests that the U.S. person being acquired provide information and classifications for any items or technology that it exports under a license granted by BIS.[185]

Separately, the EAR list specific procedures that the parties to a transaction must follow when transferring an existing license granted by BIS to a foreign party acquiring a U.S. person that exports items or technology under that license.[186] BIS reviews any such requests for transfer of a license, and the foreign acquirer must be willing and able to certify its ongoing compliance with the EAR.[187]

(2) *Military Export Controls Enforced by the U.S. Department of State*—In addition to the dual-use export controls enforced by BIS, the Department of State's Directorate of Defense Trade Controls (DDTC) enforces export controls set forth in the International Traffic in Arms Regulations (ITAR).[188] These controls restrict unlicensed exports of weapons and weapons technology, which are listed on the U.S. Munitions List (USML).[189] Given the nature of the items and technology listed on the USML, it is not surprising that the controls enforced by the DDTC are more stringent than those imposed by BIS. In addition, the ITAR require that manufacturers of defense articles and services register with the DDTC.[190]

Because of the potential national security implications of transferring military items or services to foreign countries, CFIUS carefully reviews foreign acquisitions of U.S. companies that are

registered with the DDTC or that export items listed on the USML. As noted above, the regulation that prescribes the contents of a voluntary notice to CFIUS requests information regarding any items or technology with potential military applications that the U.S. person being acquired manufactures. Specifically, the regulation asks whether the U.S. person being acquired produces defense articles and defense services under the ITAR.[191]

Apart from the CFIUS review process, the ITAR set forth a requirement that any company registered with the DDTC must notify DDTC 60 days in advance of a planned sale to a foreign person, which affords the DDTC the opportunity to object to the transaction.[192] Assuming that the DDTC does not object to the transaction, the ITAR also require a post-transaction notification in which the successor entity provides information to the DDTC to request an amendment to substitute the successor entity's name for the U.S. person's name on the U.S. person's previous registration and any export licenses.[193]

Other Related Foreign Control Issues For Government Contractors

■ Anti-Assignment Rules & Novation

Under the Anti-Assignment Act, "[t]he party to whom the Federal Government gives a contract or order may not transfer the contract or order, or any interest in the contract or order, to another party."[194] The relevant U.S. Government agency, however, may waive the effect of the Anti-Assignment Act and, at its discretion, recognize the assignment of a contract to the new entity formed as a result of the foreign acquisition.[195] Federal Acquisition Regulation (FAR) 42.1204 provides that the Government may recognize a third party as a successor in interest to the Government contract when the third party's interest arises out the transfer of (a) all of the contractor's assets or (b) the entire portion of the assets involved in performing the contract.[196] Moreover, it should be noted that transfers or assignments occurring by operation of law are exempt from the Anti-Assignment Act. For example, corporate mergers, consolidations, and reorganizations, "where in essence the contract continues with the same entity, but in a different form" are considered transfers or assignments occurring by operation of law and therefore, are not subject to the Anti-Assignment Act.[197]

Generally, a transfer of rights under an ongoing contract will "be upheld when the government recognizes it either expressly as by novations or implicitly as by ratification or waiver."[198] A novation agreement is executed by the contractor (transferor), successor in interest (transferee) and the Government, whereby the transferor guarantees performance of the contract, the transferee assumes all obligations under the contract, and the Government recognizes the transfer of the contract and related assets.[199] When a company requests a novation of its contract(s) with the Government, the contractor must submit to the Government the proposed novation agreement, as well as (1) the document describing the proposed transaction, (2) a list of all affected contracts between the contractor and the Government, (3) evidence of the third party's capability to perform, and (4) any other information requested by the Government.[200]

■ Proposal Assignment

If a company has submitted a proposal in response to a U.S. Government solicitation, but has not yet been awarded the contract, the Anti-Assignment Act does not apply. As held by the GAO, the "transfer or assignment of rights and obligations arising out of a bid or proposal is permissible where the transfer is to a legal entity which is the complete successor in interest to the bidder or offeror by virtue of merger, corporate reorganization, the sale of an entire business or the sale of an entire portion of a business embraced by the bid or proposal."[201] However, the company should be aware of any change in financial resources or performance record as a result of such transfer that may affect the Government agency's responsibility determination of the company.[202] Additionally, the Government Accountability Office (GAO) has held that, following a corporate restructuring, where the entity performing the contract is different from the entity that submitted the proposal and received

the award, that award may be overturned as it was not based on the technical approach, resources, and costs associated with the entity actually set to perform the work.[203]

■ Name Change

Even if novation of the current contract(s) is not required upon the foreign acquisition, the company and relevant Government agency will still be required to enter into a Change-of-Name Agreement if the contractor changes its name upon acquisition by the foreign interest.[204] When forwarding the executed Change-of-Name Agreement to the Contracting Officer, the company is required to submit (1) the document effecting the name change, (2) an opinion of the contractor's counsel stating that the name change was properly effected, and (3) a list of all affected contracts and purchase orders remaining unsettled between the contractor and Government.[205]

■ Conflict-Of-Interest Rules

When a company enters into negotiations with a foreign interest, the parties should investigate any potential conflict of interest that may cause the company to be disqualified from future procurements or create a conflict of interest under its ongoing contracts. FAR 9.502 provides that an organizational conflict of interest may result when "factors create an actual or potential conflict of interest on an instant contract, or when the nature of the work to be performed on the instant contract creates an actual or potential conflict of interest on a future acquisition."[206] Whether organizational conflicts of interest exist is also one of the key issues that the relevant Government agency will consider when deciding whether to allow the assignment of an ongoing contract to the new entity formed as a result of the foreign acquisition.[207]

GUIDELINES

These *Guidelines* suggest some key considerations for both parties to the transaction where there is any investment by a foreign entity in a U.S. Government contractor. They are not, however, a substitute for professional representation in any specific situation.

1. In considering whether to file a voluntary notification with CFIUS, construe the relevant factors broadly. For example, "transfer of control" should be considered to include any significant ownership interest and other indicia of control, including minority shareholder rights. "National security" should be construed broadly as well, to include critical infrastructure, law enforcement issues, antiterrorism programs, and strategic industries.

2. At the same time, identify the ownership structure of the foreign buyer, including all indirect ownership interests, including, for instance, foreign investors in funds investing in the company. It will be very important to determine the extent of all foreign government interests in the buyer.

3. Notify all interested parties, regulatory contacts, and procurement officers of the pending acquisition as soon as practicable. It will be critical to identify and address any concerns these officers may have about the acquisition because they may have the power to derail the CFIUS review process.

4. Determine whether the target maintains sensitive, classified, or export-controlled information and technologies. Does the technology require an export license (by either the Department of Commerce or the Department of State) to be transferred to the country of the buyer? If so, pay particular attention to "deemed export" concerns. There may have already been a "deemed export" violation in the context of the negotiations leading up to the deal. If so, you need to know this ahead of time.

5. Identify all contracts the target has with the DOD, the DOE, the Department of Homeland Security, or any intelligence agency. Identify and review all security clearances, facility clearances and DD254s (the DOD Contract Security classification specification form).

6. Conduct a thorough review of the export control compliance program of the target and the buyer, and put in place any necessary or

advisable improvements to integrate the target into that program.

7. Review and identify early any potential mitigation options or requirements, as well as organizational conflicts of interest. Could the surviving entity be barred from certain types of defense business? If so, what mitigation might remedy this? Determine if there are any potential conflicts of interest or restrictions on members of the proxy committee.

8. Before making the final decision to make a voluntary CFIUS notification, consider all disadvantages of making a filing, including the costs of generating the information required for the filing, making the necessary submissions, and meeting with CFIUS; the delays in the review process; the mitigation agreements CFIUS might require in return for approval of a transaction; and the risk that notification itself might raise the visibility of the transaction. Also consider whether CFIUS will be notified nonetheless as part of the NISP notification.

9. Consider how political interests, competing bidders, business rivals, or other stakeholders might attempt to kill the deal through the CFIUS process. A potential U.S. buyer may persuade the target to sell to it rather than the foreign buyer to avoid the CFIUS filing.

10. Conduct a thorough review of the export control requirements involved in the proposed transaction. Does the target have products or technologies subject to the ITAR or controlled by the Department of Commerce? Is the target registered with DDTC?

11. Consider the information disclosure requirements under the FOCI examination. Will private equity or hedge-type investors be willing and able to provide detailed information regarding the identity of foreign investors and the percentage and nature of such ownership?

12. Engage in an early dialogue with the DSS or the DOE regarding a possible change in FOCI to determine early on if the Government will have objections to the transaction or will require conditions that will significantly affect the advisability of the transaction. Utilize the existing relationship of the buyer and seller's facility security officer and the Government to facilitate a smooth transition prior to and following the transaction.

13. Advise all participants in the transaction that the Government will not provide final sign off on the novation of contracts or the mitigation of FOCI prior to closing. Be prepared to deal with potential after-the-fact adjustments to the transaction necessitated to obtain Government approval.

★ REFERENCES ★

1/ 50 U.S.C.A. app. § 2170; 31 C.F.R. pt. 800; see Order of February 1, 1990 Pursuant to Section 721 of the Defense Production Act of 1950, 55 FR 3935 (Feb. 6, 1990); Order of September 28, 2012 Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corporation, 77 Fed. Reg. 60,281 (Oct. 3, 2012).

2/ 50 U.S.C.A. app. § 2170.

3/ Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat. 1107, 1425 (1988) (adding 50 U.S.C.A. app. § 2170).

4/ Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246 (2007) (amending 50 U.S.C.A. app. § 2170).

5/ Exec. Order No. 11,858, 3 C.F.R. 990 (1971–1975), as amended by Exec. Order No. 12,188, 3 C.F.R. 131 (1981), Exec. Order No. 12,661, 3 C.F.R. 618 (1989), Exec. Order No. 12,860, 3 C.F.R. 629 (1994), Exec. Order No. 13,286, 3 C.F.R. 166 (2004), and Exec. Order No. 13,456, 3 C.F.R. 171 (2008). Executive Order 11,858 was first issued in 1975 and has been amended several times by the later Executive Orders. Executive Order 13,456 wholly amended Executive Order 11,858 in January 2008.

6/ 31 C.F.R. pt. 800.

7/ West, Lee, Brennan, Wharwood & Speice, "National Security Implications of Foreign Investment in U.S. Government Contractors," Briefing Papers No. 07-11 (Oct. 2007).

8/ Pub. L. No. 110-49.

9/ Exec. Order No. 13,456, 3 C.F.R. 171 (2008).

10/ 73 Fed. Reg. 70,702 (Nov. 21, 2008) (amending 31 C.F.R. pt. 800).

11/ Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74,567 (Dec. 8, 2008).

12/ 70 Fed. Reg. 19,467 (Apr. 9, 2014) (adding 32 C.F.R. pt. 117).

13/ 32 C.F.R. § 117.56(b)(3)(v); DOD, Directive-Type Memorandum (DTM) 09-019—"Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)" (Sept. 2, 2009), incorporating Change 6 (Jan. 9, 2014), attach.

2, at 8, available at http://www.dtic.mil/whs/directives/corres/pdf/DTM-09-019.pdf; see also DOE, Safeguards and Security Program (July 21, 2011), incorporating Change 1 (Feb. 15, 2013), app. B, sec. 2, ch. I, at I-1, available at https://www.directives.doe.gov/directives/0470.4-BOrder-b-admchg1/view (hereinafter "S&S Program").

14/ See 73 Fed. Reg. 74,567, 74,569 (Dec. 8, 2008); 31 C.F.R. § 800.601.

15/ 22 C.F.R pts.120–130.

16/ See generally West, Lee & Monahan, "U.S. Export Control Compliance Requirements for Government Contractors," Briefing Papers, No. 05-12 (Nov. 2005); Irwin, Katirai & Lorello, "Due Diligence & Compliance Risk Management Abroad for Government Contractors," Briefing Papers, No. 07-6 (May 2007); Dover, Horan & Overman, "Mergers & Acquisitions—Special Considerations When Purchasing Government Contractor Entities/Edition II," Briefing Papers, No. 09-7 (June 2009); Peters, Burgett & Sturm, "Foreign Nationals in U.S. Technology Programs: Complying With Immigration, Export Control, Industrial Security & Other Requirements," Briefing Papers No. 00-3 (Feb. 2000).

17/ Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, § 5021, 102 Stat 1107, 1425 (adding 50 U.S.C.A. app. § 2170).

18/ Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246 (2007) (amending 50 U.S.C.A. app. § 2170).

19/ 50 U.S.C.A. app. § 2170(d).

20/ 50 U.S.C.A. §§ 1701–1706.

21/ 50 U.S.C.A. app. § 2170(d)(4).

22/ 50 U.S.C.A. app. § 2170(e).

23/ Order of September 28, 2012 Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corporation, 77 Fed. Reg. 60,281 (Oct. 3, 2012).

24/ Ralls Corp. v. Comm. on Foreign Inv. in the United States, No. 12-1513 (ABJ), 2013 WL 5583847 (D.D.C. Oct. 10, 2013).

25/ 50 U.S.C.A. app. § 2170(k); Exec. Order No. 13,456, 3 C.F.R. 171 (2008).

26/ 73 Fed. Reg. 74,567, 74,568 (Dec. 8, 2008).

27/ Exec. Order No. 11,858, 3 C.F.R. 990 (1971–1975).

28/ 50 U.S.C.A. app. § 2170(k); Exec. Order No. 13,456, 3 C.F.R. 171 (2008)).

29/ Exec. Order No. 13,456, 3 C.F.R. 171 (2008).

30/ CFIUS, Annual Report to Congress, Report Period CY 2012 (Public/Unclassified Version) 3 (Dec. 2013), available at http://www.treasury.gov/resource-center/international/foreign-investment/Documents/2013%20CFIUS%20Annual%20Report%20PUBLIC.pdf (hereinafter "CFIUS CY 2012 Annual Report").

31/ CFIUS CY 2012 Annual Report 2, 19.

32/ CFIUS CY 2012 Annual Report 2, 19.

33/ CFIUS CY 2012 Annual Report 20.

34/ CFIUS CY 2012 Annual Report 2; see also Order of September 28, 2012 Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corporation, 77 Fed. Reg. 60,281 (Oct. 3, 2012). (On September 28, 2012, President Obama issued an order to block the acquisition of four U.S. wind farm project companies whose sites are within or in the vicinity of restricted air space at the Naval Weapons Systems Training Facility in Oregon by Ralls Corporation, a company owned by Chinese nationals.)

35/ CFIUS CY 2012 Annual Report 5.

36/ CFIUS CY 2012 Annual Report 5–7.

37/ CFIUS CY 2012 Annual Report 16–18.

38/ CFIUS CY 2012 Annual Report 26–28.

39/ Order of February 1, 1990 Pursuant to Section 721 of the Defense Production Act of 1950, 55 FR 3935 (Feb. 6, 1990); Order of September 28, 2012 Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corporation, 77 Fed. Reg. 60,281 (Oct. 3, 2012).

40/ 31 C.F.R. § 800.301 (examples omitted).

41/ 31 C.F.R. § 800.224.

42/ 31 C.F.R. § 800.224.

43/ 31 C.F.R. § 800.302 (examples omitted).

44/ 31 C.F.R. § 800.303.

45/ 31 C.F.R. § 800.207.

46/ See 73 Fed. Reg. 70,702, 70,704 (Nov. 21, 2008).

47/ 31 C.F.R. § 800.204.

48/ 31 C.F.R. § 800.204 provides the following exemplary factors: "(1) The sale, lease, mortgage, pledge, or other transfer of any of the tangible or intangible principal assets of the entity, whether or not in the ordinary course of business; (2) The reorganization, merger, or dissolution of the entity; (3) The closing, relocation, or substantial alteration of the production, operational, or research and development facilities of the entity; (4) Major expenditures or investments, issuances of equity or debt, or dividend payments by the entity, or approval of the operating budget of the entity; (5) The selection of new business lines or ventures that the entity will pursue; (6) The entry into, termination, or non-fulfillment by the entity of significant contracts; (7) The policies or procedures of the entity governing the treatment of non-public technical, financial, or other proprietary information of the entity; (8) The appointment or dismissal of officers or senior managers; (9) The appointment or dismissal of employees with access to sensitive technology or classified U.S. Government information; or (10) The amendment of the Articles of Incorporation, constituent agreement, or other organizational documents of the entity with respect to the matters described in paragraphs (1) through (9) above."

49/ 31 C.F.R. § 800.302(b).

50/ See examples provided in 31 C.F.R. § 800.302(b).

51/ See examples provided in 31 C.F.R. § 800.302(b).

52/ 31 C.F.R. § 800.204(c).

53/ See 73 Fed. Reg. 70,702, 70,707 (Nov. 21, 2008).

54/ 31 C.F.R. § 800.301.

55/ 31 C.F.R. § 800.226.

56/ See 73 Fed. Reg. 70,702 70,705 (Nov. 21, 2008).

57/ 31 C.F.R. § 800.216.

58/ 31 C.F.R. § 800.212(a).

59/ 31 C.F.R. § 800.212(b).

60/ 31 C.F.R. § 800.226.

61/ 50 U.S.C.A. app. § 2170(f) (as amended by Pub. L. No. 110-49, § 4, 121 Stat. 246 (2007)).

62/ Pub. L. No. 110-49, § 4 (amending 50 U.S.C.A. app. § 2170(f)).

63/ 50 U.S.C.A. app. § 2170(f)(6) (as amended by Pub. L. No. 110-49, § 4).

64/ 50 U.S.C.A. app. § 2170(a)(6) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.208.

65/ 22 C.F.R pts.120–130.

66/ 15 C.F.R. pts. 730–774.

67/ 10 C.F.R. pt. 810.

68/ 10 C.F.R. pt. 110.

69/ 31 C.F.R. § 800.209; see 7 C.F.R. pt. 331; 9 C.F.R. pt. 121; 42 C.F.R. pt. 73.

70/ 50 U.S.C.A. app. § 2170(b)(2)(B)(i)(II) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.503.

71/ 50 U.S.C.A. app. § 2170(a)(4) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.214.

72/ 50 U.S.C.A. app. § 2170(f)(9) (as amended by Pub. L. No. 110-49, § 4).

73/ 50 U.S.C.A. app. § 2170(b)(2)(B)(i)(III) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.503.

74/ Guidance Concerning the National Security Review Conducted by the Committee on Foreign Investment in the United States, 73 Fed. Reg. 74,567 (Dec. 8, 2008).

75/ 50 U.S.C.A. app. § 2170(b)(1)(C) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.401(a).

76/ 31 C.F.R. § 800.401(b).

77/ 31 C.F.R. § 800.401(c).

78/ 31 C.F.R. § 800.401(f).

79/ 31 C.F.R. § 800.401(f).

80/ 50 U.S.C.A. app. § 2170(b)(1)(E) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.502.

81/ 31 C.F.R. § 800.504.

82/ 50 U.S.C.A. app. § 2170(b)(2)(C) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.506.

83/ 50 U.S.C.A. app. § 2170(d) (as amended by Pub. L. No. 110-49, § 6).

84/ 50 U.S.C.A. app. § 2170(b)(2)(B)(i)(II) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.503.

85/ 31 C.F.R. § 800.402.

86/ 31 C.F.R. § 800.401(a).

87/ 31 C.F.R. § 800.402.

88/ 31 C.F.R. § 800.402(c)(3)(v).

89/ 31 C.F.R. § 800.402(c)(3)(iv).

90/ 31 C.F.R. § 800.402(c).

91/ 31 C.F.R. § 800.403(a)(3).

92/ 31 C.F.R. § 800.401(c).

93/ 31 C.F.R. § 800.401(c).

94/ 50 U.S.C.A. app. § 2170(b)(1)(D)(ii)–(iii) (as amended by Pub. L. No. 110-49, § 2).

95/ 50 U.S.C.A. app. § 2170(c); see 31 C.F.R. § 800.702.

96/ See 50 U.S.C.A. app. § 2170(d)(3).

97/ 31 C.F.R. § 800.801(a).

98/ 31 C.F.R. § 800.801(b).

99/ 31 C.F.R. § 800.801(c).

100/ CFIUS CY 2012 Annual Report 20.

101/ DOD, National Industrial Security Program Operating Manual, DOD 5220.22-M (Feb. 28 2006), incorporating Change 1 (Mar. 28, 2013), at ¶¶ 2-300 to 2-310, available at http://www.dss.mil/isp/fac_clear/download_nispom.html (hereinafter "NISPOM").

102/ See Exec. Order No. 13577 (June 15, 2011), 76 Fed. Reg. 35,715 (June 20, 2011).

103/ 50 U.S.C.A. app.§ 2170(b)(2)(B)(i)(III) (as amended by Pub. L. No. 110-49, § 2); see 31 C.F.R. § 800.503.

104/ 50 U.S.C.A. app. § 2170(g) and (m) (as amended by Pub. L. No. 110-49, § 7); see also CFIUS Annual Reports, available at http://www.treasury.gov/resource-center/international/foreign-investment/Pages/cfius-reports.aspx.

105/ 50 U.S.C.A. app. § 2170(m) (as amended by Pub. L. No. 110-49, § 7(b)).

106/ NISPOM ¶ 2-302.b; S&S Program, attach. 3, sec. 1, ch. VI, at VI-3 to VI-4.

107/ 32 C.F.R. § 117.56(b)(14)(viii).

108/ Exec. Order No. 12,829, 3 C.F.R. 570 (1993).

109/ 79 Fed. Reg. 19,467, 19468 (Apr. 9, 2014); NISPOM app. C, at C-2. Other agencies, including the U.S. Department of State and the National Security Agency, perform additional or separate agency-specific personnel clearance investigations. These clearances are beyond the scope of this Briefing Paper.

110/ NISPOM ¶ 1-100.

111/ These agencies are the National Aeronautics and Space Administration, the Department of Commerce, the General Services Administration, the Department of State, the Small Business Administration, the National Science Foundation, the Department of the Treasury, the Department of Transportation, the Department of the Interior, the Department of Agriculture, the Department of Labor, the Environmental Protection Agency, the Department of Justice, the Federal Reserve System, the Government Accountability Office, the U.S. Trade Representative, the U.S. International Trade Commission, the U.S. Agency for International Development, the Nuclear Regulatory Commission, the Department of Education, the Department of Health and Human Services, the Department of Homeland Security, the Federal Communications Commission, the Office of Personnel Management, the National Archives and Records Administration, and the Overseas Private Investment Corporation. NISPOM ¶ 1-103.b; DSS Industrial Security Letter ("ISL") 2013-02 (Mar. 8, 2013), available at http://www.dss.mil/documents/facility-clearances/ISL-2013-02.pdf; ISL 2013-04 (June 10, 2013), available at http://www.dss.mil/documents/isp/ISL_2013-04.pdf.

112/ 79 Fed. Reg. 19,467.

113/ The 2014 interim final rule adds these regulations as Subpart C to part 117, "Procedures for Government Activities Relating to Foreign Ownership, Control or Influence (FOCI)." Subparts A and B are reserved, suggesting that DOD is considering adding further procedures related to the NISP at a future date.

114/ 79 Fed. Reg. 19, 467, 19,469. These regulations apply to the DSS and the agencies for which it provides industrial security services. 32 C.F.R. § 117.52(a).

115/ 32 C.F.R. § 117.56(b)(5). In fact, in the justification for the interim rule, the DOD noted that "the lack of a formal, uniform process has created significant delay in the completion of National Interest Determinations (NIDs) for foreign-owned U.S. contractors." 79 Fed. Reg. 19,467, 19,469.

116/ S&S Program app. B, sec. I, ch. I, at I-1.

117/ NISPOM app. C, at C-3. Unless otherwise stated, the NISP regulations adopt the definitions included in the NISPOM. See, e.g., 32 C.F.R. § 117.53.

118/ NISPOM ¶ 2-102. The DSS will also process companies organized and existing under the laws of any of the organized U.S. territories (Guam, the Northern Marianas Islands, Puerto Rico, and the U.S. Virgin Islands) for a facility security clearance provided such companies are located in the United States or its Territorial Areas and are otherwise eligible. In addition, it will issue facility security clearances to American Indian or Alaska Native tribal entities meeting specific criteria in addition to meeting all other clearance requirements. ISL 2013-01 (Jan. 17, 2013), available at http://www.dss.mil/documents/facility-clearances/ISL-2013-01.pdf.

119/ NISPOM ¶ 2-102; S&S Program app. B, sec. 1, ch. I, at I-3.

120/ NISPOM ¶ 2-303; S&S Program app. B, sec. 2, ch. I, at I-1.

121/ NISPOM ¶ 2-100.

122/ NISPOM ¶¶ 2-200.a, 2-212; S&S Program app. B, sec. 1, ch. V.

123/ NISPOM app. C, at C-4.

124/ NISPOM ¶¶ 2-103, 2-200, 2-212.

125/ NISPOM ¶ 2-209.

126/ NISPOM ¶ 2-209.

127/ NISPOM ¶ 2-210.

128/ NISPOM ¶ 2-300.c; S&S Program app. B, sec. 2, at 2-3.

129/ NISPOM app. C, at C-3.

130/ 32 C.F.R. § 117.56(b); NISPOM ¶ 2-300.a.

131/ 32 C.F.R. § 117.56(b)(3)(E); NISPOM ¶ 2-301; see also S&S Program app. B, sec. 2, ch. I, at I-1.

132/ NISPOM ¶ 2-301; see also S&S Program app. B, sec. 2, ch. I, at I-1.

133/ 32 C.F.R. § 117.56(b)(3)(i)(A)–(H); NISPOM ¶ 2-301; see also S&S Program app. B, sec. 2, ch. I, at I-1.

134/ NISPOM ¶ 2-302.b; S&S Program, attach. 3, sec. 1, ch. VI, at VI-3 to VI-4 (The DOE regulation provides that notification of an "anticipated change" should be made when "the contractor or any of its tier parents enters into formal negotiations toward agreement, when the parties enter into a written memorandum of understanding (MOU), or in the case of financing agreements, when written application for financing is made.").

135/ See, e.g., S&S Program app. B, sec. 2, ch. III, at III-1; ISL 2009-03 (Nov. 17, 2009), available at http://www.dss.mil/documents/pressroom/ISL_2009_03_December_09.pdf.

136/ 32 C.F.R. § 117.56(b)(2)(i); NISPOM ¶ 2-300.c; see also S&S Program app B., sec. 1, ch. VIII, at VIII-1.

137/ NISPOM ¶ 2-302.b; see also S&S Program, attach. 3, sec. 1, ch. VI, at VI-1 to VI-3.

138/ 32 C.F.R. § 117.56(b)(3)(v) ("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, owning five

percent or more of the company, cannot be identified), DSS may make a determination that the company is not eligible for an FCL."); S&S Program app. B, sec. 2, ch. I, at I-1 ("In instances where the company is unable to identify a foreign owner (e.g., the participating investors in a foreign investment or hedge fund cannot be identified), DOE may determine that the company is not eligible for an FCL.").

139/ 32 C.F.R. § 117.56(b)(4)(iii)(A); NISPOM ¶ 2-303.a; S&S Program, attach. 3, sec. 2, ch. II, at II-4.

140/ NISPOM ¶ 2-303.a; S&S Program, attach. 3, sec. 2, ch. II, at II-4; DSS, Sample Board Resolution, available at http://www.dss.mil/isp/foci/foci_mitigation.html.

141/ NISPOM ¶ 2-303.a; S&S Program, attach. 3, sec. 2, ch. II, at II-4.

142/ 32 C.F.R. § 117.56(b)(4)(iii)(B)–(C); NISPOM ¶ 2-303.c; S&S Program, attach. 3, sec. 2, ch. II, at II–3 to II–4. The DOD reports that, in calendar year 2011, 5 contractors cleared by the DOD were subject to an SCA (3 Secret, 2 Top Secret) and 16 contractors were subject to an SSA (12 Secret, 4 Top Secret). 79 Fed. Reg. 19,467, 19,468.

143/ NISPOM ¶ 2-303.c; S&S Program, attach. 3, sec. 2, ch. II, at II-3 to II-4.

144/ NISPOM ¶ 2-303.c; S&S Program, attach. 3, sec. 2, ch. II, at II-3 to II-4.

145/ 32 C.F.R. § 117.56(b)(4)(iii)(B); NISPOM ¶ 2-303.c(1); S&S Program, attach. 3, sec. 2, ch. II, at II-4.

146/ DSS, Sample Security Control Agreement, available at http://www.dss.mil/isp/foci/foci_mitigation.html; NISPOM ¶¶ 2-303.c, 2-305; S&S Program, attach. 3, sec. 2, ch. II, at II-4 to II-5.

147/ NISPOM ¶ 2-303.c(1); S&S Program, attach. 3, sec. 2, ch. II, at II-4.

148/ 32 C.F.R. § 117.56(b)(4)(iii)(C); NISPOM ¶ 2-303.c(2); S&S Program, attach. 3, sec. 2, ch. II, at II-3.

149/ DSS, Sample Special Security Agreement, available at http://www.dss.mil/isp/foci/foci_mitigation.html; NISPOM ¶¶ 2-303.c; 2-305; S&S Program, attach. 3, sec. 2, ch. II, at II-3, II-5.

150/ DSS, Sample Special Security Agreement, available at http://www.dss.mil/isp/foci/foci_mitigation.html.

151/ Defined by the NISPOM and the NISP regulations to include top secret, communication security (except classified keys used for data transfer), restricted data, special access program, and sensitive compartmented information. NISPOM ¶ 2-303.c(2), n.1; 32 C.F.R. § 117.53.

152/ 32 C.F.R. § 117.56(b)(5); NISPOM § 2-303.c(2); S&S Program, attach. 3, sec. 2, ch. II, at II-3.

153/ NISPOM ¶ 2-303.c(2)(b); see also 32 C.F.R. § 117.56(b)(14)(vi).

154/ 32 C.F.R. § 117.56(b)(10)(ii); NISPOM ¶ 2-308; S&S Program, app. B, sec. 2, ch. III, at III-2 to III-3.

155/ 32 C.F.R. § 117.56(b)(4)(iii)(D); NISPOM ¶ 2-303.b; S&S Program, attach. 3, sec. 2, ch. II, at II-2 to II-3. The DOD reports that, in calendar year 2011, there were no VTAs and nine PAs. 79 Fed. Reg. 19,467, 19.468.

156/ NISPOM ¶ 2-303.b; S&S Program, attach. 3, sec. 2, ch. II, at II-2 to II-3.

157/ NISPOM ¶ 2-303.b; S&S Program, attach. 3, sec. 2, ch. II, at II-2 to II-3.

158/ NISPOM ¶ 2-303.b; S&S Program, attach. 3, sec. 2, ch. II, at II-2 to II-3.

159/ 32 C.F.R. § 117.56(b)(4)(iii)(D).

160/ NISPOM ¶ 2-303.b(1); S&S Program, attach. 3, sec. 2, ch. II, at II-2 to II-3, II-5.

161/ NISPOM ¶ 2-305.b; S&S Program, attach. 3, sec. 2, ch. II, at II-5.

162/ NISPOM ¶ 2-303.b(1); S&S Program, attach. 3, sec. 2, ch. II, at II-2 to II-3.

163/ 32 C.F.R. § 117.56(b)(10)(ii); NISPOM ¶ 2-308.

164/ NISPOM ¶ 2-309; S&S Program app. B, sec. 1, ch. IV, at IV-1 to IV-2; see also 32 C.F.R. § 117.56(b)(13).

165/ NISPOM ¶ 10-102.b.

166/ NISPOM ¶ 10-102.a.

167/ NISPOM ¶ 2-309; S&S Program app. B, sec. 1, ch. IV, at IV-1 to IV-2.

168/ DSS, Affiliated Operations Plan, http://www.dss.mil/isp/foci/affiliated-operations-plan.html; see also DSS, Affiliated Operations Plan Template, available at http://www.dss.mil/isp/foci/affiliated-operations-plan.html.

169/ DSS, Affiliated Operations Plan, http://www.dss.mil/isp/foci/affiliated-operations-plan.html; see also DSS, Affiliated Operations Plan Template, available at http://www.dss.mil/isp/foci/affiliated-operations-plan.html.

170/ DSS, Facilities Location Plan, http://www.dss.mil/isp/foci/foci_collocation.html; see also DSS, Facilities Location Plan Template, available at http://www.dss.mil/isp/foci/foci_collocation.html.

171/ DSS, Facilities Location Plan, http://www.dss.mil/isp/foci/foci_collocation.html; see also DSS, Facilities Location Plan Template, available at http://www.dss.mil/isp/foci/foci_collocation.html.

172/ 32 C.F.R. § 117.56(b)(7); NISPOM ¶ 2-306.c; S&S Program, attach. 3, sec. 2, ch. II, at II-6; DSS, Technology Control Plan, http://www.dss.mil/isp/foci/technology-control-plan.html; see also DSS, Sample Technology Control Plan, available at http://www.dss.mil/isp/foci/technology-control-plan.html.

173/ 32 C.F.R. § 117.56(b)(8); DSS, Electronic Communications Plan, http://www.dss.mil/isp/foci/elec_com.html; see also DSS, Electronic Communications Plan Template, available at http://www.dss.mil/

isp/foci/elec_com.html; DSS, Electronic Communications Plan Sample, available at http://www.dss.mil/isp/foci/elec_com.html.

174/ DSS, Visitation Plan, http://www.dss.mil/isp/foci/visitation.html.

175/ 31 C.F.R. pts. 500–598. See generally Irwin, Katirai, & Lorello, supra note 14, at 4–6.

176/ See 31 C.F.R. pts. 535, 560, 561, 562.

177/ See 31 C.F.R. pt. 515.

178/ See 31 C.F.R. pt. 510.

179/ E.g., 31 C.F.R. § 538.211 (prohibiting evasion of the sanctions enforced against Sudan); see also Low & McGlone, "Avoiding Problems Under the Foreign Corrupt Practices Act, U.S. Antiboycott Laws, OFAC Sanctions, Export Controls, and the Economic Espionage Act," in Negotiating and Structuring International Commercial Transactions 206–07 (Sandstrom & Goldsweig eds., 2d ed. 2003).

180/ E.g., 31 C.F.R. § 538.206 (prohibiting facilitating violations of the sanctions enforced against Sudan); see also Low & McGlone, "Avoiding Problems Under the Foreign Corrupt Practices Act, U.S. Antiboycott Laws, OFAC Sanctions, Export Controls, and the Economic Espionage Act," in Negotiating and Structuring International Commercial Transactions 206 (Sandstrom & Goldsweig eds., 2d ed. 2003).

181/ 31 C.F.R. § 800.402(c)(1)(iii), (v), (vi).

182/ See generally Irwin, Katirai & Lorello, "Due Diligence & Compliance Risk Management Abroad for Government Contractors," Briefing Papers, No. 07-6 (May 2007).

183/ 15 C.F.R. pts. 730–774. See generally West, Lee & Monahan, "U.S. Export Control Compliance Requirements for Government Contractors," Briefing Papers, No. 05-12 (Nov. 2005).

184/ 31 C.F.R. § 800.402(c)(5)(ii).

185/ 31 C.F.R. § 800.402(c)(4)(i).

186/ 15 C.F.R. § 750.10.

187/ 15 C.F.R. § 750.10.

188/ 22 C.F.R. pts. 120–130. See generally West, Lee & Monahan, "U.S. Export Control Compliance Requirements for Government Contractors," Briefing Papers, No. 05-12 (Nov. 2005).

189/ 22 C.F.R. pt. 121.

190/ 22 C.F.R. pt. 122.

191/ 31 C.F.R. § 800.402(c)(4)(ii).

192/ 22 C.F.R. § 122.4(b).

193/ 22 C.F.R. § 122.4(c).

194/ 41 U.S.C.A. § 6305(a).

195/ Maffia v. United States, 143 Ct. Cl. 198, 203 (1958) ("Despite the bar of the Anti-Assignment statute ([then codified at] 41 U.S.C.A. § 15), the Government, if it chooses to do so, may recognize an assignment").

196/ FAR 42.1204(a).

197/ Westinghouse Elec. Co. v. United States, 56 Fed. Cl. 564, 569 (Fed. Cl. 2003), 45 GC ¶ 251; see also Johnson Controls World Servs., Inc. v. United States, 44 Fed. Cl. 334 (Fed. Cl. 1999).

198/ Westinghouse Elec. Co. v. United States, 56 Fed. Cl. at 569.

199/ FAR 2.101.

200/ FAR 42.1204(e).

201/ Sunrise Int'l Group, Inc., Comp. Gen. Dec. B-266357, 96-1 CPD ¶ 64; Harnischfeger Corp., Comp. Gen. Dec. B-224371, 86-2 CPD ¶ 296.

202/ Consortium HSG Technischer Serv. GmbH and GeBe Gebäude-und Betriebstechnik GmbH Südwest Co., Mgmt. KG, Comp. Gen. Dec. B-292699.6, 2004 CPD ¶ 134.

203/ Wyle Laboratories, Inc., Comp. Gen. Dec. B-408112.2, 2014 CPD ¶ 16, 56 GC ¶ 39. In this decision, the GAO considered an award made to Science Applications International Corporation (SAIC) following a corporate restructuring that split SAIC into two separate companies. Although the GAO noted that SAIC had fully disclosed this restructuring to the Government in the original proposal, and that the Government understood the change in corporate structure, it nonetheless overturned the award to "new" SAIC determining that the agency had evaluated only the proposal of "old" SAIC, and thus failed to provide adequate support and a reasonable basis for its award.

204/ FAR 42.1205.

205/ FAR 42.1205(a).

206/ FAR 9.502(c). See generally Cairnie & Kessler, "Organizational Conflicts of Interest/Edition V," Briefing Papers No. 12-13 (Dec. 2012).

207/ FAR 42.1204(d).