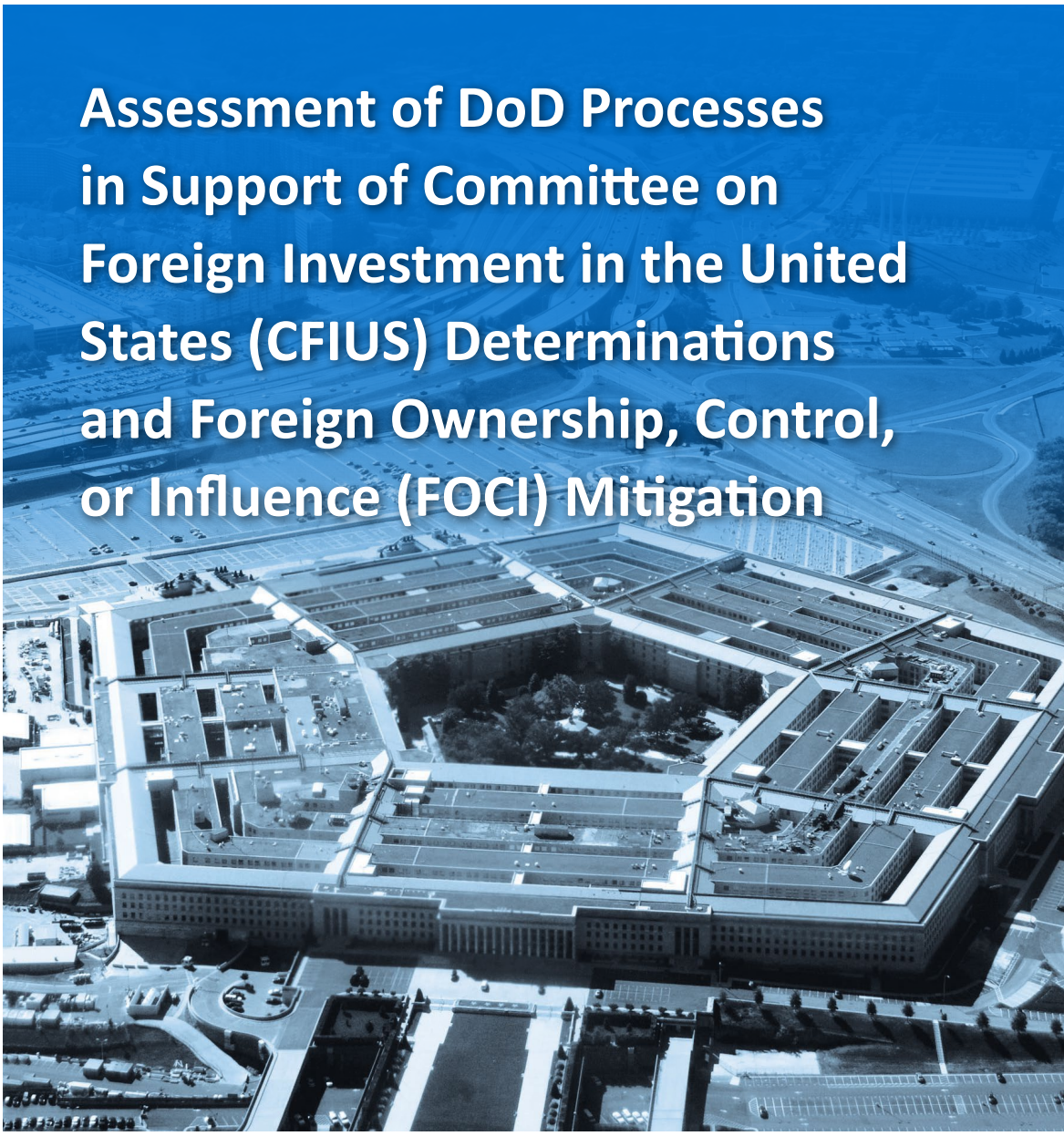
Report No. DODIG-2014-080

INSPECTOR GENERAL

U.S. Department of Defense

JUNE 10, 2014

Assessment of DoD Processes in Support of Committee on Foreign Investment in the United States (CFIUS) Determinations and Foreign Ownership, Control, or Influence (FOCI) Mitigation



INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

INTEGRITY ★ EFFICIENCY ★ ACCOUNTABILITY ★ EXCELLENCE

Mission

Our mission is to provide independent, relevant, and timely oversight of the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; advises the Secretary of Defense and Congress; and informs the public.

Vision

Our vision is to be a model oversight organization in the Federal Government by leading change, speaking truth, and promoting excellence—a diverse organization, working together as one professional team, recognized as leaders in our field.

Fraud, Waste, & Abuse
HOTLINE
Department of Defense
dodig.mil/hotline

For more information about whistleblower protection, please see the inside back cover.

Results in Brief

Assessment of DoD Processes in Support of Committee on Foreign Investment in the United States (CFIUS) Determinations and Foreign Ownership, Control, or Influence (FOCI) Mitigation

June 10, 2014

Objective

This report on the assessment of DoD processes to support Committee on Foreign Investment in the United States (CFIUS) determinations and foreign ownership, control, or influence (FOCI) mitigation responds to longstanding management concerns and the U.S. Government Accountability Office (GAO) high risk area of ensuring the effective protection of technologies critical to U.S. national security interests.

We assessed the process for determining and relaying relevant threat information and recommendations to the CFIUS, the strength of FOCI mitigation within cleared defense industry, and the effectiveness of existing tools to help FOCI mitigations and CFIUS determinations.

Findings

We found that existing policies clearly define requirements to support National Interest Determinations, but they do not effectively delineate roles and responsibilities to support the Services, agencies, and the acquisition community resulting in a significant backlog of decisions.

We also found that a need exists for a centralized, accessible database to process and store DD Form 254s—a document that

Visit us at www.dodig.mil

Findings (cont'd)

specifies security requirements for classified contracts—as part of an enterprise system that manages the flow of contract information to support industrial security within cleared defense industry.

Recommendations

We recommend that the Under Secretary of Defense for Intelligence (USD(I)), in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), issue guidance that defines ownership of information, delineates responsibility for coordination within respective Service and agency organizations, and outlines a consistent process flow for National Interest Determinations to further a synchronized, integrated approach to support CFIUS determinations and foreign ownership, control, or influence mitigation. We further recommend that the USD(I), in coordination with the USD(AT&L), direct the creation of a centralized repository for cleared defense contracts, to maintain DD Form 254s and other contract security requirements for classified contracts, and designate the Defense Security Service as executive agent in its role as the National Industrial Security Program Cognizant Security Office for DoD, 26 non-DoD agencies, and approximately 13,500 cleared contractors.

Management Comments

Management concurred with the two main recommendations and its comments were responsive. Management non-concurred with designating at this time an executive agent for the DD Form 254 central repository. We require no further comment and will continue to monitor DD Form 254 repository developments, along with the corresponding Office of Management and Budget/Federal Register approval process.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Under Secretary of Defense for Acquisition, Technology, and Logistics		A, B
Under Secretary of Defense for Intelligence		A, B

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

June 10, 2014

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE
DIRECTOR, DEFENSE SECURITY SERVICE

SUBJECT: Assessment of DoD Processes in Support of Committee on Foreign Investment in the United States (CFIUS) Determinations and Foreign Ownership, Control, or Influence (FOCI) Mitigation (Report No. DoDIG-2014-080)

We are providing this report for your information and use. We issued a draft of this report on February 10, 2014. This report responds to a request by a former Under Secretary of Defense for Intelligence, to assess the efficacy of FOCI mitigation within the defense industrial base and review the process for relaying relevant information to the CFIUS. It also responds to the U.S. Government Accountability Office high risk area of "ensuring the effective protection of technologies critical to U.S. national security interests."

We considered comments from the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, and the Office of the Under Secretary of Defense for Intelligence. Management concurred with the two main recommendations and its comments were responsive. Management non-concurred with designating at this time an executive agent for the DD Form 254 central repository. We require no further comment and will continue to monitor DD Form 254 repository developments, along with the corresponding Office of Management and Budget/Federal Register approval process.

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 882-4860, or the Project Manager at (703) 699-7214 (DSN 499-7214).

Anthony C. Thomas
Deputy Inspector General for
Intelligence and Special
Program Assessments

Distribution:

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense for Intelligence
Director, Defense Security Service
Director, Missile Defense Agency
Assistant Secretary of the Army for Acquisitions, Logistics and Technology
Army Deputy Chief of Staff, G-2
Assistant Secretary of the Air Force for Acquisition
Administrative Assistant to the Secretary of the Air Force
Assistant Secretary of the Navy for Research, Development, and Acquisition
Deputy Under Secretary of the Navy for Plans, Policy, Oversight and Integration

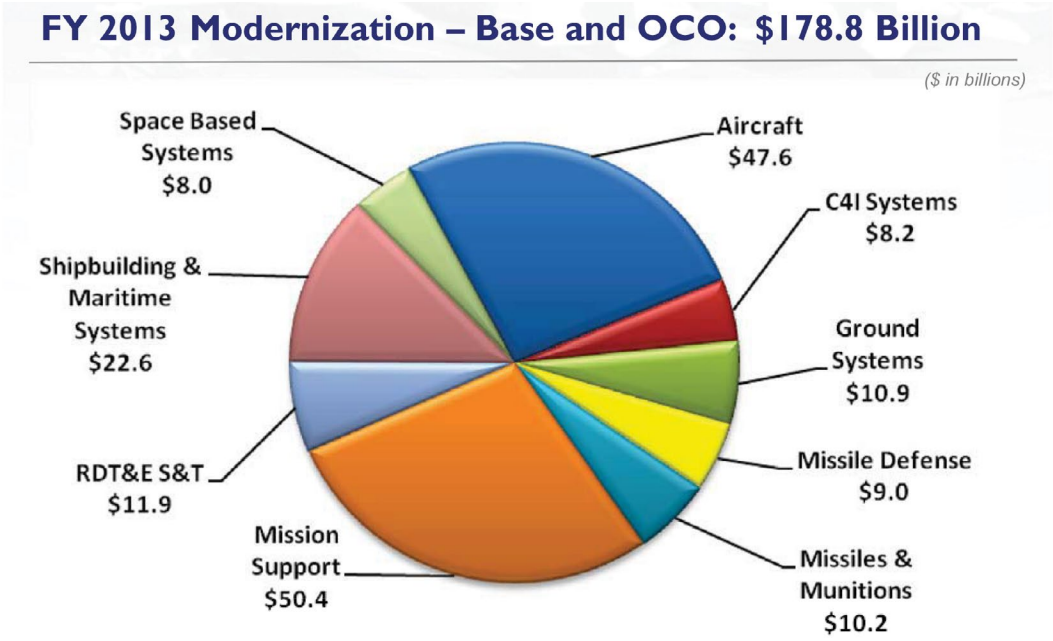
Contents


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Introduction

To compete in a global economy, the United States must foster an environment that encourages foreign investments. Foreign investments can increase a nation's gross domestic product, with a corresponding increase in labor productivity, wages, and employment. The United States is the world's leader in attracting foreign direct investments. Such foreign investments are not risk-free, as they can potentially result in unauthorized access to classified or sensitive information or adversely affect the performance on classified or unclassified contracts within the defense industrial base.[1] Accordingly, the United States must engender an environment that encourages foreign investments while protecting information vital to national security. These competing requirements should be considered when mitigating Foreign Ownership, Control, or Influence (FOCI) within cleared defense industry,[2] and reviewing industry mergers and acquisitions that are under Committee on Foreign Investment in the United States (CFIUS) purview.

Major Weapons Systems FY 2013 Funding Requests



Source: FY2013 PRCP – Investment Categorization
Numbers may not add due to rounding

[1] The defense industrial base is the DoD, government, and private sector worldwide industrial complex capable of performing research and development, and designing, producing, and maintaining military weapon systems, subsystems, components, or parts to meet military requirements.

[2] Cleared defense industry is the DoD, government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. Cleared defense industry does so in accordance with requirements established in the National Industrial Security Program Operating Manual (NISPOM).

DoD's FY 2013 acquisition funding request for weapons development, research, and sustainment totaled about $178.8 billion. DoD, through the Defense Security Service (DSS), also provides for reviewing FOCI concerns and administering mitigation instruments for cleared defense industry—an essential partner in systems development.

In addition, DoD, as a member of CFIUS, supports CFIUS determinations in two ways. First, through its intelligence components, DoD provides threat information to the Office of the Director of National Intelligence (ODNI), which develops the aggregate threat assessment for each CFIUS case. Second, DoD provides risk analyses which assess threat, vulnerability, and overall risk including proposals to mitigate risks for those companies where DoD equities require the analyses and proposals. This report reviews the FOCI and CFIUS processes to determine whether roles and responsibilities are clearly defined, whether these efforts are sufficiently synchronized and integrated in DoD, and whether additional tools are needed to help bring about a consistent, comprehensive approach to FOCI mitigation and CFIUS determinations.

Objective

This report responds to a request by a former Under Secretary of Defense for Intelligence, to assess the efficacy of FOCI mitigation within the defense industrial base and review the process for relaying relevant information to the CFIUS. It also responds to the U.S. Government Accountability Office (GAO) high risk area of "ensuring the effective protection of technologies critical to U.S. national security interests." Thus, this report assesses:

- The process for determining and relaying relevant threat information on a CFIUS transaction from the appropriate DoD intelligence agency to the DoD CFIUS lead and to the ODNI office responsible for the aggregate intelligence community position on threats posed by a CFIUS case;
- The efficacy of FOCI mitigation within cleared defense industry; and,
- The effectiveness of existing tools to support FOCI mitigation under the National Industrial Security Program Operating Manual (NISPOM), which in turn, is a contributing factor to CFIUS determinations when companies being acquired possess facility clearances.

Background

A U.S. company is considered to fall under FOCI when a foreign interest has the power to direct or decide matters affecting that company's managing of operations in a way that may result in unauthorized access to classified information or cause an adverse effect on the performance of classified contracts.

It applies whether this power is direct or indirect, whether or not it is exercised, and whether or not it is exercisable through owning the U.S. company's securities by contractual agreement or other means.

FOCI considerations of U.S. companies requiring access to classified information are explicitly addressed in the NISPOM, which the Secretary of Defense is responsible for issuing and maintaining. FOCI concerns are one element to consider during the CFIUS review process. DoD supports these programs through the synchronized efforts of its security, intelligence, and counterintelligence communities coordinating with the defense acquisition community.

FOCI policy is an element of the National Industrial Security Program (NISP). The policy was designed to ensure that classified information in the custody of cleared U.S. companies is protected from unauthorized access if a cleared U.S. company is or will be acquired, controlled, or influenced by foreign interests. When a cleared defense company is considered to be under FOCI, the U.S. company is ineligible for a facility security clearance unless and until security measures (e.g., certain mitigation instruments) have been installed to negate or mitigate the FOCI. Similarly, CFIUS—an interagency committee—reviews mergers and acquisitions involving a foreign individual, corporation, or other entity as a buyer to determine the effect of such transactions on national security. In 2011, CFIUS reviewed 111 voluntarily-filed proposed mergers or acquisitions.

The Department of the Treasury serves as the CFIUS chair, with the other statutory members consisting of the Departments of Justice, Homeland Security, Commerce, Defense, State, and Energy, the Office of the U.S. Trade Representative, and the Office of Science and Technology Policy.

By Executive Order, the President has added other Executive Office agencies as participants on the Committee, including the Office of Management and Budget, the Council of Economic Advisors, and the National Security Staff. The Director of National Intelligence (DNI) and the Secretary of Labor are non-voting, ex-officio members.

While CFIUS and FOCI determinations under NISP authorities proceed along separate but parallel tracks, support for the programs is becoming increasingly coordinated and integrated. The primary difference between the determinations from an industry perspective is that for cleared defense industry, compliance with FOCI reporting is mandatory under NISP authorities, while the reporting to CFIUS of planned or completed mergers or acquisitions is voluntary (although CFIUS does have the authority to request notices and member agencies have the authority to file notices). Therefore, cleared defense contractors must report changed ownership conditions (i.e., "change conditions") to the DSS. The DSS reviews those required change-condition reports to determine if the degree of FOCI presented by the change requires carrying out a FOCI agreement or requires any modifications to an existing FOCI mitigation or negation agreement. In contrast, CFIUS can only review mergers and acquisitions when a foreign entity could subsequently exert control of a business engaged in U.S. interstate commerce, filing a formal notice with CFIUS is primarily voluntary by firms involved in mergers and acquisitions and CFIUS action to impose mitigation measures or recommend Presidential action on a transaction is discretionary.

Relevant FOCI Policies

The primary authorities that provide for reviewing cleared defense contractors for FOCI concerns are found in three separate issuances:

- Executive Order (E.O.) 12829, "National Industrial Security Program," January 6, 1993, which established the NISP (E.O. 12829 was amended by E.O. 12885 of December 16, 1993);
- DoD Manual 5220.22, Chapter 2, "Security Clearances," Section 3 "Foreign Ownership, Control or Influence" of the NISPOM, which identifies the criteria for FOCI's existence, establishes the requirements for annual reviews of companies under FOCI, and details the forms and certifications that address contractors' operating requirements; and,
- Directive-Type Memorandum (DTM) 09-019, "Policy Guidance for Foreign Ownership, Control, or Influence," September 2, 2009, which provides further guidance on FOCI mitigation procedures, allows for greater coordination on CFIUS matters, summarizes DoD policies, and clarifies requirements for National Interest Determinations (NIDs).[3] The current DTM incorporates Change 6 of January 9, 2014.

[3] A NID is a determination from a Government Contracting Activity that access to proscribed information is consistent with U.S. national security interests.

Executive Order 12829

Issued on January 6, 1993, E.O. 12829 established the NISP with the goal to protect classified information that is released to contractors, licensees, and grantees of the U.S. Government. E.O. 12829 stated that issuing contracts to non-governmental organizations promotes national interests, but can result in contractor access to classified information. For this reason, E.O. 12829 stipulates that classified information released to contractors must be protected at levels commensurate with those in the Federal Government. E.O. 12829 also stated national security requires that an industrial security program promote U.S. economic and technological interests without redundancy or unnecessary requirements. Accordingly, this E.O. designated the NISP as the "single, integrated, cohesive industrial security program to protect classified information and to preserve our Nation's economic and technological interests." To that end, it specified creating the NISPOM to "prescribe specific requirements, restrictions, and other safeguards" for the handling of classified information.

National Industrial Security Program Operating Manual

Established in 1993 by E.O. 12829, the NISPOM regulates protecting classified information within cleared defense industry. The NISPOM stipulates the procedures and requirements for government contractors, concerning managing and protecting classified information within the defense industrial base. The requirements are detailed in the NISPOM, which lists four Cognizant Security Agencies (CSAs)—the Departments of Defense and Energy, the Central Intelligence Agency, and the Nuclear Regulatory Commission. The 2006 NISPOM also lists 23 non-DoD agencies that have agreements with the Secretary of Defense to render industrial security services as the Executive Agent for the NISP.

Since 2006, DoD has also entered into agreements with three other non-DoD agencies for a total of 26. Guidance with respect to FOCI is found in Chapter 2 (see "Relevant FOCI Policies") of the NISPOM. The section details requirements for annual reviews of companies under FOCI and details the forms and certifications that address contractors' operating requirements.

The NISPOM was amended in March 2013 to reflect changes which included carrying out the provisions of Executive Order 13526, "Classified National Security Information," December 29, 2009, regarding derivative classifier identification and training.

This amendment identified the authority of the DNI and acknowledged that intelligence information is under DNI jurisdiction and control. The DNI establishes security policy for protecting intelligence information, sources, methods, and analytical processes.

Directive-Type Memorandum (DTM) 09-019

Additional guidance for FOCI mitigation was issued in DTM 09-019, a memorandum that details procedures and requirements and allows for greater coordination on CFIUS matters. It reconfirms the standards for FOCI's existence, specifies timelines to U.S. companies to appeal FOCI determinations, and says: "DSS shall also obtain and consider counterintelligence and technology transfer risk assessments from all appropriate USG sources." The DTM also provides guidance with regard to NIDs, stipulating that when a foreign interest intends to merge with or acquire a cleared company with access to proscribed information, the government contracting activity shall review the FOCI action plan that the company proposed. A NID is required if a Special Security Agreement (SSA) is used to mitigate FOCI. DSS advises the Government Contracting Activities (GCA) regarding the need for a NID and the GCA determines whether a NID will be issued. A Deputy Secretary of Defense memorandum provides further guidance and additional requirements regarding the processing of NIDs.

Key Stakeholder – FOCI

Defense Security Service (DSS)

The DSS is a Defense agency under USD(I) authority, direction, and control that serves as the DoD NISP Cognizant Security Office, providing industrial security oversight and support to Defense agencies, the Services, 26 non-DoD federal agencies, and approximately 13,500 cleared contractor facilities. The organization's core operational elements are the Center for Development of Security Excellence, Industrial Policy and Programs, Industrial Security Field Operations, and Counterintelligence.

In accordance with these responsibilities, DSS inspects, monitors, and provides assistance to the contractors, licensees, and grantees that require access to classified information.

An April 2008 GAO report entitled "Department of Defense – Observations on the National Industrial Security Program" discussed the DoD NISP and identified areas for improvement related to FOCI. Specific to FOCI, the report identified the following:

- concerns with how DSS collects and analyzes information needed to assess oversight of both contractor facilities and contractors under FOCI;
- the lack of guidance to DSS field staff to effectively provide oversight at contractor facilities under FOCI; and,
- the delay between cleared defense companies entering into foreign business transactions and the reporting of such to DSS.

Since the report's release, DSS has staffed analytical, assessment and evaluation, and operational offices to provide continuous monitoring of more than 10,000 cleared companies for change conditions, such as foreign acquisitions and provide proactive support for FOCI mitigation and oversight for more than 350 cleared companies operating under FOCI mitigation agreements. DSS also reviews and monitors financial data to determine financial viability, foreign indebtedness, foreign capital contribution, and to compare company-reported information against commercial financial databases. In addition, DSS' analytical elements communicate change conditions to DSS oversight personnel through the NISP Facility Oversight weekly newsletter designed to increase awareness of change conditions within the NISP. Finally, DSS has instituted operational procedures for FOCI that identify responsibilities and provide for a consistent process to support the field elements in FOCI determinations and oversight within cleared defense industry.

Companies entering into the NISP are required to complete a Standard Form-328 (SF-328), "Certificate Pertaining to Foreign Interest," to report the extent of foreign ownership, control, or influence within their businesses. Companies self-report any change conditions to FOCI factors in accordance with the NISPOM and a clarifying Industrial Security Letter.

In May 2009, DSS conducted a beta test where FOCI analysts reviewed all SF-328 forms for companies entering into the NISP regardless of company responses. The review revealed concerns that FOCI was underreported. For this reason, DSS now reviews all SF-328s and conducts independent analysis to validate the information that prospective cleared companies provide.

During fiscal year 2012, DSS reviewed SF 328s for over 1,500 companies. Of those reviews, about nine percent of the companies in-process for a facility clearance (FCL)[4] had unreported FOCI issues, and five percent had counterintelligence issues. Depending upon the nature and extent of the FOCI issues identified, DSS can require one of several mitigation instruments to minimize the risk of unauthorized disclosure of classified information.

Distinct mitigation instruments are executed for corresponding levels of assessed risk. The first, a Board Resolution, is instituted when a foreign investor has a minority stake, is not a member of the governing board, and is not authorized to appoint or elect board members. A board resolution is a legally binding document from the organization's governing board acknowledging the foreign investors identified from the first phase of the FOCI process. The resolution prevents foreign investors from having unauthorized access to classified, or export-controlled information,[5] and denies influence or control over projects involved with classified information. Another mitigation instrument called a Security Control Agreement is typically imposed for minority foreign ownership when the foreign owner does not effectively own or control the business and is entitled to representation on the cleared company's board. The foreign owner is permitted to retain a limited voice in managing the business, but is precluded from unauthorized access to classified or export-controlled unclassified information.

A Special Security Agreement is a mitigation agreement that may be used when a foreign entity effectively owns or controls a company, and, as a result, the SSA has more security restrictions than a Security Control Agreement.

[4] A facility clearance or FCL is an administrative determination that, from a national security standpoint, a facility is eligible for access to classified information at the same or lower classification category as the clearance being granted. The FCL may be granted at the Confidential, Secret, or Top Secret level. The FCL includes the execution of a Department of Defense Security Agreement (DD Form 441). Under the terms of the agreement, the Government agrees to issue the FCL and inform the contractor as to the security classification of information to which the contractor will have access. The contractor, in turn, agrees to abide by the security requirements set forth in the NISPOM.

[5] Unclassified information, the export of which is controlled by the International Traffic in Arms Regulations ("ITAR") and/or the Export Administration Regulations ("EAR"). The export of technical data, which is inherently military in nature, is controlled by the ITAR. The export of technical data, which has both military and commercial uses, is controlled by EAR.

The SSA still allows the foreign owner a voice in the business management through representation on the company's governing board via one or more Inside Directors, directors representing the interests of the foreign entity. However, the SSA also requires a minimum of three Outside Directors (or a number greater than the number of Inside Directors) to act on the government's behalf.

Outside Directors are independent directors nominated by the foreign interest and approved by DSS which do not have any personal or professional relationships to the parties of the FOCI mitigation agreement. An SSA requires the following:

- a Technology Control Plan—a security countermeasure that stipulates how a company will prescribe measures to control access to non-U.S. citizen employees and visitors to information for which they are not authorized;
- an Electronic Communications Plan—which supports the separation of networks and provides assurance that electronic communications do not result in the unauthorized disclosure of classified or export-controlled information or exert undue influence over the company; and
- a visitation policy—which outlines how visits from the foreign entity will be controlled by the cleared company.

Additional mitigation instruments include Proxy Agreements and Voting Trust Agreements, which are more restrictive than other mitigation agreements and do not require a NID for a cleared company to have contracts requiring access to proscribed information that include: Top Secret information; Communications Security information except controlled cryptographic items when either unkeyed or used with unclassified keys; Special Access Program information; Sensitive Compartmented information; and Restricted Data. This report will focus on SSAs, and, in some cases, the resulting need for NIDs.

DSS is responsible for negotiating, executing, and administering mitigation instruments in cleared defense industry and for making recommendations to the OUSD(I) on whether FOCI mitigation is adequate to address any national security concerns for those CFIUS cases involving cleared defense contractors. In both cases, when an SSA mitigation instrument is in place and the company requires access to proscribed information, DSS shall advise the GCAs of the need for a NID. In addition to GCA approval, concurrence from owners of the proscribed information (i.e. the National Security Agency for Communications Security information, the Department of Energy for Restricted Data, and the ODNI for Sensitive Compartmented Information) must be obtained.

Relevant CFIUS Policies

CFIUS reviews mergers, acquisitions, or takeovers that may result in "foreign control of any person engaged in interstate commerce in the United States" (it may also consider whether the transaction could result in control of any "critical infrastructure" that could impair national security). These transactions are defined as covered transactions and were defined as such in the Exon-Florio provision, which is further detailed below. This report summarizes the following CFIUS laws, regulations, and guidance:

- E.O. 11858, "Foreign Investment in the United States," May 7, 1975;
- The Exon-Florio Amendment to the Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100-418, 102 Stat. 1107, "Authority to Review Certain Mergers, Acquisitions, and Takeovers," USC 50 App § 2170, which established Presidential authority to block proposed mergers and acquisitions;
- Public Law 110-49, "Foreign Investment and National Security Act," July 26, 2007, which formally established CFIUS under statute and clarified the process for national security reviews; and,
- DoD Instruction 2000.25, "DoD Procedures for Reviewing and Monitoring Transactions Filed with the Committee on Foreign Investment in the United States (CFIUS)," August 5, 2010, which provides internal DoD guidance to support CFIUS.

Executive Order 11858

In establishing CFIUS, E.O. 11858 authorized the Secretaries of State, Treasury, Defense, and Commerce, and the U.S. Trade Representative, the Chairman of the Council of Economic Advisers, the Attorney General, and the Director of the Office of Management and Budget to serve as committee members, with the Secretary of Treasury as committee chair. The committee's primary responsibility is to monitor foreign investment in the United States by analyzing trends and developments.

The committee is also tasked to provide guidance and review investments with possible major implications for U.S. national interests, and submit coordinated Executive Branch recommendations and analyses to the National Security Council and the Economic Policy Board, as warranted.

Exon-Florio Amendment

Enacted under the Omnibus Trade and Competitiveness Act of 1988, the Exon-Florio Amendment modified Section 721 of the Defense Production Act of 1950 by establishing an investigative process to determine the effects on national security of proposed mergers, acquisitions, and takeovers of U.S. companies by foreign interests. The Exon-Florio provision gave a maximum of 90 days to finish reviewing a proposed transaction. The decision to investigate had to be made within 30 days. If so determined, a subsequent investigation had to be completed in 45 days. The President had to decide within an additional 15 days whether action was to be taken to block the transaction. These timelines remain in effect.

The President designated CFIUS to administer the Exon-Florio amendment in E.O. 12661, Section 3-201: "Implementing the Omnibus Trade and Competitiveness Act of 1988 and Related International Trade Matters" of December 27, 1988. With the Exon-Florio amendment, Congress authorized the President to review foreign acquisitions, mergers, or takeovers of U.S. companies including defense-related firms. The President gained the authority to suspend or prohibit such transactions if they presented "credible evidence" of threats to national security which could not be addressed by other laws.

Foreign Investment and National Security Act

Public Law 110-49, 50 United States Code, Appendix 2061, the Foreign Investment and National Security Act (FINSA) was signed into law July 26, 2007, and added additional requirements to the Exon-Florio Amendment. Previously operating under the authority of E.O. 11858, CFIUS was also formally established in statute under FINSA. The Secretary of Energy was added as a voting member and the Secretary of Labor and the DNI were added as non-voting members. Under FINSA, the DNI is tasked to analyze the threat to the national security of the United States posed by a covered transaction, and incorporate the views of intelligence agencies regarding these threats, although it is statutorily constrained not to contribute to any subsequent policy discussions in CFIUS. The Act requires that for each covered transaction, at least one member of CFIUS will be designated as a co-lead agency with Treasury. The duties of the co-lead agency(ies) include negotiating, modifying, monitoring, and enforcing any agreement CFIUS enters

into with foreign persons in order to mitigate national security risks. FINSA also provides CFIUS the authority to impose mitigation measures during a CFIUS investigation period without Presidential approval if the parties fail to agree to terms the Committee considers necessary to protect national security.

The Act also stipulates that the designated lead agency continue to monitor mitigation instruments that they enter into on behalf of the Committee. While notifying CFIUS about a transaction remains voluntary, FINSA formalized the process which allows for unilateral initiating of reviews by CFIUS absent an industry filing. Moreover, FINSA stipulates that approved transactions can be undone if material information was found to have been deliberately withheld or misrepresented during the review.

DoD Instruction 2000.25

DoD Instruction 2000.25 establishes policy, assigns responsibilities, and provides instructions for DoD CFIUS reviews and designates primary responsibility for oversight of these efforts to the Under Secretary of Defense for Policy. However, in 2011, the Secretary of Defense directed that the lead DoD responsibility for CFIUS be transferred to the Under Secretary of Defense for Acquisition, Technology, and Logistics.

The instruction also establishes the DoD CFIUS Monitoring Committee and prescribes procedures to both propose mitigation agreements that are then recommended to CFIUS, as well as monitor those agreements that CFIUS approves and the parties sign. It assigns responsibilities to over 20 DoD organizations, departments, and component heads to review and monitor CFIUS transactions where DoD equities exist and establishes internal timelines for CFIUS reviews that ensure compliance with Committee requirements.

The instruction stipulates that the DoD CFIUS process should be transparent, to the extent possible. It also says organizations should address potential implications for relevant DoD programs, assets, and future technological superiority resulting from a foreign acquisition involving a defense supplier, defense-related technologies, and infrastructure critical for DoD missions. The instruction further directs DoD Components that are members of the Intelligence Community to fulfill their alternate role of providing additional support and information to the ODNI regarding threats that CFIUS transactions pose.

Key DoD Stakeholders – CFIUS

Office of the Under Secretary of Defense for Acquisitions, Technology, and Logistics

As previously noted, as part of the DoD Efficiencies Review, the Office of the Secretary of Defense transferred DoD lead responsibility for CFIUS to the USD(AT&L), with the change becoming effective in October 2011. The primary CFIUS responsibility within the Office of the USD(AT&L) was delegated to the office of the Deputy Assistant Secretary for Manufacturing and Industrial Base Policy (MIBP). In this capacity, MIBP serves as the DoD representative to CFIUS, negotiates agreements with industry, and internally negotiates and prepares the DoD position on CFIUS matters.

Office of the Under Secretary of Defense for Intelligence

When acquisitions and mergers involve cleared defense contractors under DSS oversight, the members of CFIUS understand that DSS evaluates FOCI mitigation options under its NISP authorities. DoD does advise CFIUS of the results of the DSS FOCI mitigation determination. However, apart from the role that DSS plays in determining if FOCI mitigation is feasible under NISPOM guidance and the particular form it should take, CFIUS members are also responsible for determining if CFIUS mitigation is required to protect national security for those parts of a transaction which are not covered by NISPOM authorities over classified contracts.

Operating under OUSD(I) authority, direction, and control, DSS coordinates proposed FOCI mitigation under NISP authorities through the OUSD(I). DSS gives a consolidated OUSD(I) response to USD(AT&L) on mergers and acquisitions that are subject to the FOCI program of the NISPOM and that also meet the definition of a covered transaction under CFIUS. DSS also provides valuable information to USD(AT&L) and CFIUS on FOCI mitigation and also briefs CFIUS on FOCI issues.

If after reviewing a case, DSS determines an acceptable level of FOCI mitigation and the GCA also finds the FOCI level acceptable, this information is reported to the OUSD(AT&L)/MIBP through OUSD(I). If DSS needs more time to complete its FOCI review than the 30 days afforded under the parallel CFIUS review, OUSD(I) requests a CFIUS investigation to enable DSS to complete its FOCI decision process in time for the responsible DoD officials to complete their CFIUS consideration within CFIUS statutory deadlines.

In either case, CFIUS, as a group, must still conclude whether the FOCI mitigation negotiated by those member agencies with classified contracts is adequate to address any identified national security concerns and meet the statutory CFIUS clearance standard of no unresolved national security concerns.

Services

As the main source of classified contracts within DoD, the Services play an integral role in both CFIUS and FOCI determinations. As the GCA, the appropriate Service will receive communications with the filings attached from both the OUSD(AT&L)/MIBP and DSS if the transaction involves a cleared company advising of CFIUS notifications by companies under their purview and the parties' FOCI mitigation proposal respectively.

The Services review the information and submit their concurrence or non-concurrence within the prescribed timeframes by the DoD CFIUS lead and DSS for DTM 09-019. When the proposed merger or acquisition involves cleared defense industry, established guidelines exist for the mitigation required under the FOCI authorities from DTM 09-019. However, determining whether appropriate CFIUS mitigation measures are required depends on the broader facts and circumstances of each case, and DoD components combine their respective assessments and make recommendations as part of the overall CFIUS review process, which considers the adequacy of existing law to address identified national security risks.

In addition, one Service acquisition official said the Services need to better understand what the Office of the Secretary of Defense expects the Services to provide for a CFIUS review. He also said his office would appreciate standardizing the process to ensure that expectations are being met.

Missile Defense Agency

The Missile Defense Agency (MDA) International Security office is the designated lead for engaging appropriate MDA organizations that are accountable for reviewing, coordinating, and processing CFIUS cases. That office chairs the MDA CFIUS Coordination Team, which is supported by General Counsel; the Director, Research Development and Acquisition; Security; and a representative and an alternate from the Contracting Directorate, Special Programs; and the Counterintelligence Division.

The office has an internal 13-day timeline for processing CFIUS cases and for formulating and presenting MDA's position. CFIUS cases that have MDA equities are reviewed and evaluated using an established procedure that ensures a comprehensive review for identifying any MDA concerns. The cases are coordinated with other stakeholder Staff Directorates, and recommendations are formulated based on security evaluations and input received during the coordination process. MDA's recommendations are forwarded to OUSD AT&L for consolidating into a DoD position.

Defense Intelligence Agency

DoD Instruction 2000.25 charges the Director, Defense Intelligence Agency (DIA) with providing analytical support to DoD-related CFIUS determinations. In turn, the Director, DIA, delegated the responsibility to the Office of Technology and Long-Range Analysis, which provides risk assessments for mergers and acquisitions with DoD equities. The information is provided internally to the Office of the Secretary of Defense for inclusion in a broader security threat assessment that the CFIUS group within the National Intelligence Council prepares. The Council supports the Director of National Intelligence as the head of the Intelligence Community and its center for long-term strategic analysis. At DIA, the Technology and Long-Range Analysis office prepares assessments that determine the technology transfer and diversion risks of CFIUS transactions based on specific criteria. Of note, however, is that while the office does provide analytical input, it does not offer recommendations on approving proposed mergers or acquisitions.

Finding A

DoD Policy Must Clearly Define NID Roles and Responsibilities

The Deputy Secretary of Defense memorandum, "Improving the Implementation of Policy Guidance for Foreign Ownership, Control, or Influence (FOCI)" of September 14, 2011, established requirements to ensure that GCAs make timely submissions of NIDs to authorize foreign-owned or controlled U.S. companies cleared under (or in process for a facility clearance under) an SSA access to proscribed information. Despite this memorandum, a persistent backlog of NIDs exists within some Services and organizations. This is due, in part, to existing security policy and guidance which, while establishing time requirements, does not provide for a consistent process among Services and organizations. The resulting backlog can delay facility clearances and may impede technically proficient foreign-owned U.S. companies from fully participating in the government contracting process.

Determinations require coordination among internal DoD security, intelligence elements, and GCAs, and both internal and external government owners of proscribed information. For this reason, it is essential that DoD establish consistent processes DoD-wide. This will help ensure interagency coordination to bring about timely responses regarding NIDs.

The NID Process Through NISP Authorities

National Interest Determinations are an integral part of the FOCI program under NISP authorities. This holds true when classified contracts involve proscribed information[6] and the decision whether to pursue a NID, along with an SSA will also affect the recommendations that DSS, OUSD(I), and the affected GCAs will make to the DoD CFIUS lead. When a cleared U.S. company performing on an existing classified contract with access to proscribed information is acquired by a foreign interest, or when a U.S. company cleared under an SSA wants to bid on a new contract requiring such access to proscribed information, DTM 09-019 directs DSS to advise the affected GCA that it requires a NID. The requirement for NIDs

[6] Proscribed information includes Top Secret; Communications Security material, excluding Controlled Cryptographic Items when unkeyed or utilized with unclassified keys; Restricted Data; Special Access Program; and Sensitive Compartmented Information.

applies to new contracts pending issuance to existing SSA companies, and also to existing contracts when foreign interests acquire cleared companies and an SSA is the proposed mitigation.

Once the decision is made that a NID is required, DSS will alert the GCA of that requirement. The GCA, in turn, will determine which office has authority over the contract and seek the necessary concurrences. DSS can supply threat or FOCI information to help an organization assess associated risk. An overarching policy exists on requiring NID decisions within 30 days (allowing an additional 30 days for NIDs requiring coordination with concurring agencies, i.e., National Security Agency for COMSEC, Department of Energy for Restricted Data, or the ODNI for Sensitive Compartmented Information), but current processes and guidance do not support the timelines associated with the policy. After the GCAs coordinate the prepared NID for signature within their respective organizations, the signed NID is forwarded to DSS, and DSS notifies the SSA company that the NID has been awarded. The complete NID package must include a security point of contact, but it also must be signed off at the acquisition-program executive-office level.

Deputy Secretary of Defense National Interest Determination Memorandum

The Deputy Secretary of Defense signed the NID memorandum to address the persistent backlog of pending NIDs. The memorandum cited the "slow, inconsistent, and often unresponsive consideration of national interest determinations (NIDs) by government contracting activities (GCAs)." Accordingly, each DoD component head was required to provide the name of a senior official (e.g., senior acquisition executive or component equivalent), who would be responsible and have the authority to make NID decisions for the component. Component heads were advised that the names had to be provided to the USD(AT&L), USD(I) and the Director, DSS, within 30 days of the memorandum's date. The Deputy Secretary of Defense also stipulated that monthly reports be sent to the USD(I) and the USD(AT&L) on all pending NID requests more than 30 days old. He said that the report would include the status of all NIDs awaiting concurrence from non-DoD owners of proscribed information. When the memo was issued, about 300 unresolved determinations existed from current foreign owned companies operating under DSS approved SSAs.

The Deputy Secretary of Defense charged GCAs to resolve the backlog within 60 days of the memorandum date. A NID status summary report from September 14, 2012—slightly more than a year after the issuance of the memo—listed 179 pending determinations from GCAs, with 31 requiring input from the owners of proscribed information (concurring agencies). The average length of time pending for GCAs was 458 days; the average length of time for input from concurring agencies was 278 days.

Identified Concerns

The Deputy Secretary of Defense memorandum on NID procedures sought to ensure timeliness and accountability for determinations by requiring the designation of a responsible senior official and submitting recurring reports detailing metrics for outstanding NIDs. The memorandum did not, however, establish a standardized process for the Services and organizations. The definition of a senior official is not clearly articulated. For example, the individual can either be a "senior acquisition executive" or a "component equivalent." This ambiguity of what qualifies as a component equivalent prevents standardizing a process that involves elements both internal and external to DoD. Of note, minutes from a February 2012 NID working-group meeting indicated that despite the September 2011 memorandum, several organizations had yet to identify a senior official. Accordingly, a follow-on memorandum was being sent to those GCAs who had not formally responded with a point of contact. The level of GCA non-compliance indicates that a standardized process among organizations is absent.

Information obtained via interviews with officials charged with supporting CFIUS determinations confirmed the need for a standardized approach for NIDs under NISP authorities. One official said that the process is "broken" and that some of the Services used "outdated NID procedures." It was also said that the information owners or concurring agencies often disregard NID requests instead of giving a timely response. One Service security official said a central issue is the absence of an identified line of communication between the security and acquisition sides to support the NID process. Without a central "belly button," no way exists to ensure the timely exchange of information. The Deputy Secretary of Defense memorandum does not specify that the designated senior official should be affiliated with security or acquisition; thus, the memorandum fails to address this concern.

As the primary GCAs, the Services periodically encounter issues when determining which office has authority for specific contracts. A Navy security official discussed the Navy's internal NID process. When security officials are notified that a NID is needed, they must find the appropriate acquisition office with cognizance over the contract. However, the contract can at times be joint, or under the aegis of multiple organizations. Therefore, determining the responsible party can be difficult. Also, the contract could be close to expiring, e.g., within the next three months, or already expired. In such cases, some acquisition personnel choose not to respond to the determination request because it has become irrelevant, or soon will be.

Successful Practices (Army)

Of all the Services, the Army had the greatest success coordinating the efforts of its intelligence, security, and acquisition communities. More specifically, the Army has ensured timely responses from owners of proscribed information to support NIDs. This was accomplished when elements within Army Industrial Security and Counterintelligence underwent an independent process review to determine areas for improvement within its CFIUS program. The resulting changes included identifying and training additional personnel and creating checklists, standard operating procedures, and documented workflows. In addition, a CFIUS case quality tracker was created to track deficiencies, and quality and completeness issues were communicated to external DoD organizations. Internal communication was also improved by creating an inter-departmental governance structure. For areas where the concern involved resource constraints, the Army identified low-cost workflow management technology options.

The Army created checklists to ensure that requests to owners of proscribed information had the requisite data for information owners to submit responses without having to request additional information, thus proactively preventing delays in NID processing under NISP authorities. Furthermore, the Army created template memos for respective owners of proscribed information, draft justifications for information owner determinations, and examples of determinations to be forwarded to DSS. The Army G-2 worked diligently to be the focal point for all NIDs and end the NID backlog. DSS sends the initial NID request to the Army G-2 and the Army G-2 would determine what Army element was responsible. The Army G-2 tracked all the NIDs in a database until a final NID determination was made and forwarded to DSS. The Army G-2 also collaborated with the Command and Industrial Security personnel to explain the NID process and due dates.

While the new procedures played a major role in ensuring the timely processing of NIDs, Army G-2 also noted the presence within the Army acquisition office of "champions" who improve communication between G2 and the Assistant Secretary of the Army for Acquisition, Logistics, and Technology. This advancement, along with education and training, are ways in which the Army has managed to achieve effective coordination between Army G-2 and Acquisition elements.

The Army is currently transferring primary responsibility for CFIUS issues to its acquisition office, with direct support from the Deputy Assistant Secretary of the Army (Procurement) contract office. This is consistent with changes at the Office of the Secretary of Defense-level where OUSD AT&L MIBP has the lead for CFIUS matters. Moreover, because acquisition and contract offices are more readily able to identify responsible parties for NIDs under NISP authorities and for CFIUS reviews, the change should ensure continued timely processing of CFIUS cases. This change will also include continued coordination with Army G-2 and its Counterintelligence and Industrial Security elements. A chart detailing the coordinated efforts within the Army in support of CFIUS, as well as established timelines, is shown on Appendix B.

Current Efforts

The Government Industrial Security Working Group (GISWG) has also focused on issues related to delays in NID processing. The GISWG is a government working group that DSS chairs. It meets quarterly, or on an as-needed basis to address relevant security policy implementation related to industrial security matters. An October 2012 presentation at the GISWG stated that NIDs have been a topic of discussion for the GISWG and DoD for several years. The briefing referenced the Deputy Secretary of Defense memorandum on NIDs and acknowledged that despite the guidance, a backlog of over a year persists for some determinations.

To address this problem, the GISWG established a separate working group to discuss creating "blanket" NIDs, or NIDs that authorize a scope of information broader than traditional NIDs, which are program, project, or contract specific. The working group, comprised of DoD, DSS, and concurring agencies established procedures and conditions for a limited blanket NID concurrence. Limited blanket NID concurrence will cover specific categories of proscribed information and enable approval for entire companies that meet specified criteria. The company must show a history of no International Traffic in Arms Regulations violations, and compliance with an SSA for a minimum of 10 years.

In addition, a threat assessment, a FOCI assessment, and an annual security vulnerability assessment must be in place. The company or the GCA can originate the request for a blanket NID concurrence. Additional criteria exist for applicants and once granted, companies will be required to maintain a "Satisfactory" or higher security rating.

Conclusion

The Deputy Secretary of Defense memorandum sought to address "the slow, inconsistent, and often unresponsive consideration of national interest determinations (NIDs) by government contracting activities (GCAs)." Data from DSS and GISWG meeting minutes, however, show that a significant backlog of determinations still exists within some organizations. The persistent delays that remain in NID processing affect industry, the Services, organizations, and DoD headquarters.

While the limited blanket NID concurrence will improve coordination issues with owners of proscribed information, it will not remedy incongruous DoD internal processes of GCAs. The issue of inconsistent NID processes within DoD Services and organizations can, and should be, addressed at the DoD headquarters level.

Recommendation, Management Comments, and Our Response

Recommendation A

We recommend that the Under Secretary of Defense for Intelligence, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics, issue guidance that both delineates responsibility for coordination within respective Services and organizations, and outlines a consistent process flow for NIDs to further a synchronized and coordinated approach to support CFIUS determinations and FOCI mitigation.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence concurred with our recommendation and stated that a proposed directive-type memorandum is in the DoD policy issuance process. The proposed directive-type memorandum is expected to be approved and published by the third quarter of FY 2014.

Our Response

The comments of the Under Secretary of Defense for Intelligence were responsive.

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics also concurred with our recommendation.

Our Response

The comments of the Under Secretary of Defense for Acquisition, Technology, and Logistics were responsive.

Finding B

DoD Needs A Centralized and Transparent Contractor Database

DoD elements involved in identifying and carrying out security requirements presently have limited access to the information necessary to support industrial security. This is due, in no small part, to the absence of a central repository for classified contracts and relevant documentation. The result is a cumbersome and inefficient process to verify, track, and manage relevant contractor documentation. A centralized database will help ensure consistent and coordinated efforts in DoD.

DD Form 254

DD Form 254, "DoD Contract Security Classification Specification," is a security-requirements document associated with the NISP. A DD Form 254 must be included in any contract that requires access to classified information and is issued by a DoD component or Executive Branch Department or Agency that has an agreement with DoD. At the time of preparing this report, 26 federal agencies have such agreements with DoD. DD Form 254 details for the contractor the relevant security provisions required for protecting classified information accessed, generated, received, or otherwise associated with the contract. It also establishes the scope of a contractor's security program. In addition, the form provides the framework for the required DSS oversight of the contractor's security program. A copy of DD Form 254 is provided in Appendix C.

Some information provided in the DD Form 254 is captured in the DSS Electronic Facility Clearance (e-FCL) system. Currently, all companies in process for a FCL or reporting a change condition are entered into e-FCL, which functions as a central repository of company information required for FCLs and FOCI mitigation. DSS is able to upload forms related to FOCI mitigation to include the mitigation agreement and its implementation procedures into e-FCL.

The system also retains relevant corporate information, which includes articles of incorporation and bylaws, key management personnel lists, shareholder agreements, certificates of incorporation, SF-328 "Certificate Pertaining to Foreign Interest," DD Form 441 "Department of Defense Security Agreement," and DD Form 254.

Presently, 65 percent of cleared contractors under DSS security cognizance have accounts in the e-FCL system. Regarding contractor-completed DD Form 254s, the system does not correlate the information entered with other systems because it is not an enterprise database. Accordingly, data is only as accurate as the information that is received.

Identified Concerns

DSS has identified several issues on how DD Form 254 and contractor information is processed. The absence of a central repository for classified contracts and relevant documentation results in limited access and visibility for the offices tasked with identifying and carrying out security requirements associated with those contracts. Before being entered into the e-FCL, DD Form 254s are received in either paper or PDF format and either faxed, emailed, or hand-carried to the appropriate offices. Identified issues include timeliness, accuracy, absence of verification of receipt, and lack of version control. The lack of an automated centralized process for creating, submitting, reviewing, modifying, approving and/or reapproving, and storing DD Form 254 results in a cumbersome, inefficient, and often ineffective process.

DSS documents also identify concerns with how DD Form 254s are currently managed. Absent oversight for quality control, no means exist to prevent or reduce human errors or redundancies. No means are currently in place to ensure data integrity, visibility, and access control of the information contained in DD Form 254. While the information is unclassified, it is still important that the information contained therein be protected.

While forms reside with the contractor, DD Form 254s are also sometimes distributed by the GCA to the DSS office with authority over the contractor. This distribution may include many organizations in support of the contract, including Program Managers, Prime Contractors, Subcontractors, GCAs, and the DSS field office with oversight of the contractor facility. The approximately 13,500 cleared contractor facilities over which DSS has oversight retain copies of the form—one per classified contract. Larger companies can have thousands of classified contracts.

Once received by DSS, the forms may be retained in paper or PDF format in one of the 26 field office locations in separate facility file folders. GCAs may find it difficult to determine the appropriate DSS field office for receipt of the form, particularly for multiple-facility organizations where contract performance may occur at a division office, subsidiary, or cleared offsite location.

Moreover, the relationships of cleared facilities within a corporate family can be difficult to ascertain, making it hard to track a classified contract/program from a prime contractor through the various tiers of subcontractors. Consequently, no efficient comprehensive process exists to track government programs or technologies across the defense industrial base, and no mechanism exists for searching DD Forms 254 based on user-defined criteria.

The concerns listed above are also reflected in comments that the Services and organizations expressed identifying specific problems accessing or validating information provided on the DD Form 254.

During the award of classified subcontracts, cleared prime contractors occasionally enter inconsistent requirements (e.g., the need to have access to COMSEC) and that information is not vetted through a central repository or a granting agency. This can add unnecessary upfront security costs and subsequently delay NIDs if a company incorrectly identifies requirements upfront for an SSA company, resulting in later requests for determinations from uninvolved information owners. Both Services and organizations identified the inconsistency of information provided in DD Form 254s. While the information is submitted in a standardized form, it is not always correctly filled out. It was also pointed out that USD(AT&L) had "scrambled" to meet time requirements for two CFIUS cases as a result of information that contractors had misidentified in boxes on DD Form 254.

A related issue was also raised involving uncleared subcontractors, whose business information is not listed in any type of industrial security repository. Such subcontractors with significant foreign revenue or foreign connections could present a FOCI concern if they are in the supply chain for components of classified technology. The issue of uncleared subcontractors within the cleared contractor supply chain surfaced several times and warrants a separate in-depth review to determine potential supply-chain risks to cleared defense industry.

While no direct prohibition to using the DD Form 254 exists for unclassified contracts, the purpose of the form and its data collection is for contracts requiring access to classified information, as outlined in the Federal Acquisition Regulation.

Current Efforts

GISWG meeting minutes, additional documents, and interviews reveal that the feasibility of creating a Contract Security Classification Specification/DD Form 254 database has been discussed for several years. The project, however, has never been funded. The Army G-2 developed such a database to support its own sensitive compartmented information contracts, and the Army Acquisition element has a database of unclassified contracts. No centralized DD Form 254 database exists, however, for all DoD elements and the NISP. The Army's sensitive compartmented information database was reviewed to determine if it could serve as a model for a database to support DoD and NISP. It was decided that the database contained elements which could provide the foundation for a similar database supporting all DD Form 254 documentation. A demonstration of the Army system was provided to stakeholders to include all of the DoD components, Executive Branch Agencies, cleared contractors, OUSD(I), and the Information Security Oversight Office. A decision was made that the Army system could be modified to fulfill the greater need of the NISP. The DSS Office of the Chief Information Officer has initiated a project to use the Army system as the basis for a contract security requirements specification database. The intent is to collect requirements from the various stakeholder groups pending contract efforts to secure a requirements-definition subject-matter expert. Requirements-definition workshops will then be established with various stakeholder groups.

Conclusion

A single repository for security specifications for classified contracts (e.g., DD Form 254s) within DoD, and within the cleared contractor community, can provide centralized access and visibility to all parties involved in the NISP. GCA can enter security specifications directly into the database at the beginning of the acquisition process, thereby reducing the likelihood that inaccurate and potentially unnecessary costly requirements will be added. Cognizant elements could have 24-hour access to their respective DD Form 254s via controlled access and role-based permissions. A centrally-managed database will help track

the status of DD Form 254 through the life of the contract process, while also improving quality and consistency via an automated creation, review, and approval process. It will also help in analyzing security trends among Government projects and programs.

At issue is whether Acquisition or Security will have accountability for the DD Form 254 database and the resulting enterprise system. Given its existing relationship with cleared defense industry, and its role in administering the NISP on behalf of the Secretary of Defense and user agencies, DSS is well-positioned to provide oversight for any resulting database and, as previously noted, is actively working to create a functioning database upon which an enterprise system could ultimately be constructed.

Recommendation, Management Comments, and Our Response

Recommendation B

We recommend that the Under Secretary of Defense for Intelligence, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics, direct the creation of a centralized repository for cleared defense contracts, to maintain DD Form 254s and other contract security requirements for classified contracts, and designate the Defense Security Service as executive agent in its role as the National Industrial Security Program Cognizant Security Office for DoD, 26 non-DoD agencies, and approximately 13,500 cleared contractors.

Under Secretary of Defense for Intelligence Comments

The Under Secretary of Defense for Intelligence concurred with the first part of our recommendation to direct the creation of a centralized repository for cleared defense contracts, to maintain DD Form 254s and other contract security requirements for classified contracts. They stated that ongoing efforts by the Defense Security Service for developing the National Industrial Security Program Contract Classification System—the single repository for contract security classification specifications to support DoD and the National Industrial Security Program—began in 2012. Further, the DoD Investment Review Board is evaluating the National Industrial Security Program Contract Classification System and the Review Board's approval is necessary before the Defense Security Service can obligate any funds to build the National Industrial Security

Program Contract Classification System. The Defense Security Service is also working with the Defense Procurement and Acquisition Policy Office, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, to determine the possibility of co-developing the National Industrial Security Program Contract Classification System. Developing this system will reduce design and development lag time by leveraging an existing Under Secretary of Defense for Acquisition, Technology, and Logistics database.

The Under Secretary of Defense for Intelligence did not concur with the last portion of our recommendation that requested the designation of the Defense Security Service as executive agent in its role as the National Industrial Security Program Cognizant Security Office for DoD, 26 non-DoD agencies, and approximately 13,500 cleared contractors. They stated that in coordination with OUSD(AT&L) they will reevaluate whether there is a requirement for an executive agent, during the development of the National Industrial Security Program Contract Classification System as well as the Office of Management and Budget/ Federal Register information collection approval process. The Under Secretary of Defense for Intelligence anticipates approval of a revised DD Form 254 information collection with DoD's updated industrial security policy in the second quarter of FY 2015.

Our Response

The comments of the Under Secretary of Defense for Intelligence were responsive to the recommendation. We will monitor the development of the DD Form 254 central repository, and the corresponding Office of Management and Budget/Federal Register approval process, to determine the feasibility of an appointment. Otherwise, the response of the Under Secretary of Defense for Intelligence addressed all the specifics of the recommendation, and no additional comments are required.

Under Secretary of Defense for Acquisition, Technology, and Logistics Comments

The Under Secretary of Defense for Acquisition, Technology, and Logistics quoted the Under Secretary of Defense for Intelligence response to this recommendation, agreeing to the first portion of Recommendation B to direct the creation of a centralized repository for cleared defense contracts, to maintain DD Form 254s

and other contract security requirements for classified contracts. They non-concurred with the portion of the recommendation to designate the Defense Security Service as executive agent for the National Industrial Security Program Contract Classification System.

Our Response

The comments of the Under Secretary of Defense for Acquisition, Technology, and Logistics were responsive to the recommendation to create a centralized repository for cleared defense contracts. We will monitor the development of the DD Form 254 central repository, and the corresponding Office of Management and Budget/Federal Register approval process, to determine the feasibility of an appointment. Otherwise, the response of the Under Secretary of Defense for Intelligence addressed all the specifics of the recommendation, and no additional comments are required.

Appendix A

Scope and Methodology

This assessment was conducted from April 2012 to July 2013, in accordance with Quality Standards for Inspection and Evaluation that the Council of the Inspectors General on Integrity and Efficiency issued. Those standards require that we plan and perform the assessment to obtain sufficient appropriate evidence to provide a reasonable basis for our findings and conclusions based on our assessment objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our assessment objectives. To accomplish the objective, we reviewed relevant policies and guidance and interviewed officials responsible for carrying out FOCI mitigation and DoD support to CFIUS determinations.

Computer-Processed Data

We did not use computer-processed data to perform this assessment.

Use of Technical Assistance

We did not receive any technical assistance for this assessment.

Prior Coverage

During the last five years, the DoD OIG has issued no reports that have addressed issues specific to FOCI and CFIUS concerns. Unrestricted DoD OIG reports are at http://www.dodig.mil.

GAO

During the last five years, the GAO issued the following two reports addressing issues specific to FOCI and CFIUS concerns:

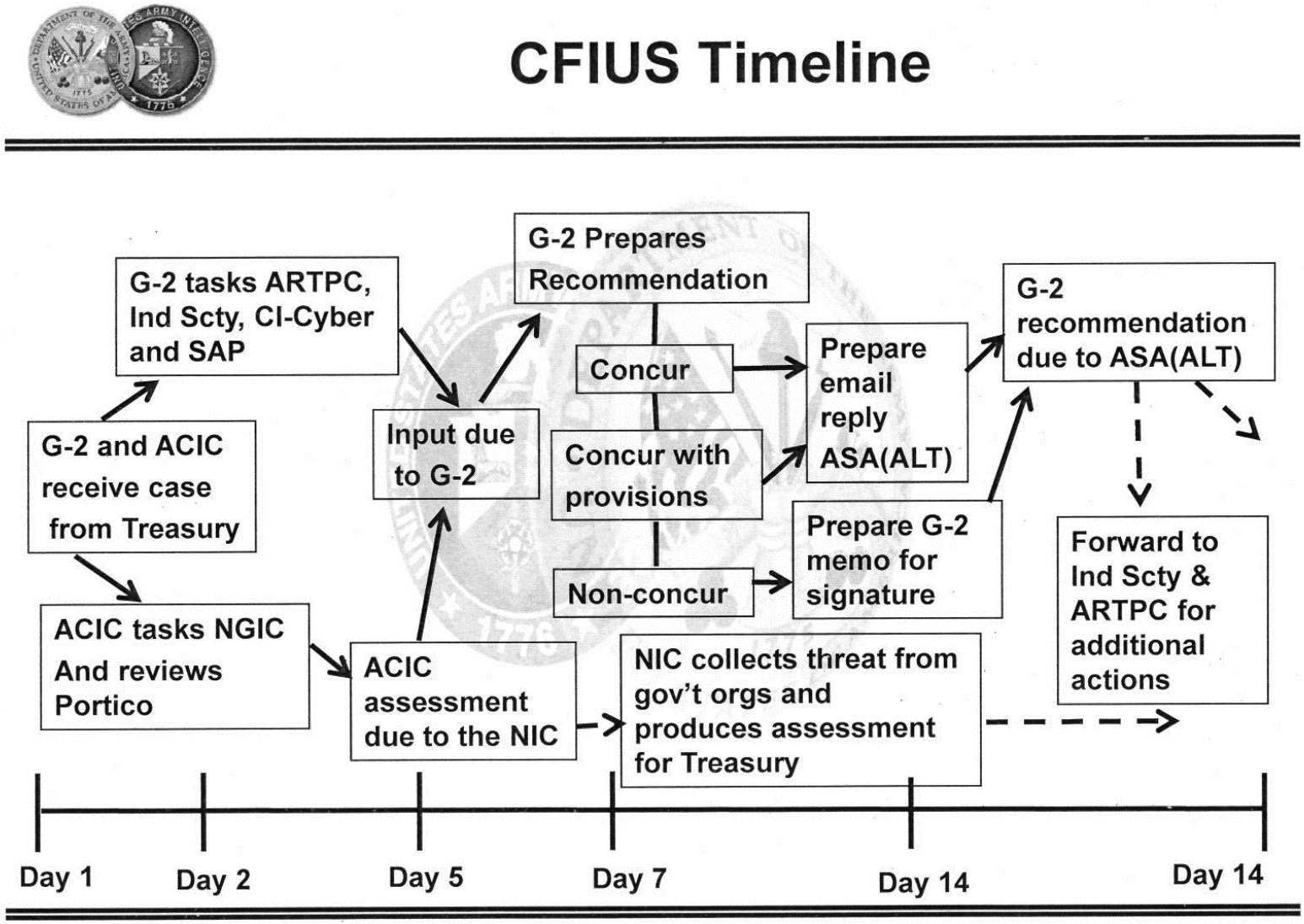
GAO Report No. GAO-08-0695T, "Department of Defense: Observations on the National Industrial Security Program," April 2008.

GAO Report No. GAO-08-0320, "Foreign Investment: Laws and Policies Regulating Foreign Investment in 10 Countries," February 2008.

Unrestricted GAO reports are at http://www.gao.gov.

Appendix B

G-2 CFIUS Timeline



Appendix C

DD Form 254

DEPARTMENT OF DEFENSE
CONTRACT SECURITY CLASSIFICATION SPECIFICATION
(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)

1. CLEARANCE AND SAFEGUARDING
a. FACILITY CLEARANCE REQUIRED
b. LEVEL OF SAFEGUARDING REQUIRED

2. THIS SPECIFICATION IS FOR: *(X and complete as applicable)*			3. THIS SPECIFICATION IS: *(X and complete as applicable)*		
	a. PRIME CONTRACT NUMBER			a. ORIGINAL *(Complete date in all cases)*	DATE *(YYYYMMDD)*
	b. SUBCONTRACT NUMBER			b. REVISED *(Supersedes all previous specs)* REVISION NO.	DATE *(YYYYMMDD)*
	c. SOLICITATION OR OTHER NUMBER	DUE DATE *(YYYYMMDD)*		c. FINAL *(Complete Item 5 in all cases)*	DATE *(YYYYMMDD)*

4. IS THIS A FOLLOW-ON CONTRACT? ☐ YES ☐ NO. If Yes, complete the following:
Classified material received or generated under _____ *(Preceding Contract Number)* is transferred to this follow-on contract.

5. IS THIS A FINAL DD FORM 254? ☐ YES ☐ NO. If Yes, complete the following:
In response to the contractor's request dated _____, retention of the classified material is authorized for the period of _____

6. CONTRACTOR *(Include Commercial and Government Entity (CAGE) Code)*

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

7. SUBCONTRACTOR

a. NAME, ADDRESS, AND ZIP CODE	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

8. ACTUAL PERFORMANCE

a. LOCATION	b. CAGE CODE	c. COGNIZANT SECURITY OFFICE *(Name, Address, and Zip Code)*

9. GENERAL IDENTIFICATION OF THIS PROCUREMENT

10. CONTRACTOR WILL REQUIRE ACCESS TO:	YES	NO	11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	YES	NO
a. COMMUNICATIONS SECURITY (COMSEC) INFORMATION			a. HAVE ACCESS TO CLASSIFIED INFORMATION ONLY AT ANOTHER CONTRACTOR'S FACILITY OR A GOVERNMENT ACTIVITY		
b. RESTRICTED DATA			b. RECEIVE CLASSIFIED DOCUMENTS ONLY		
c. CRITICAL NUCLEAR WEAPON DESIGN INFORMATION			c. RECEIVE AND GENERATE CLASSIFIED MATERIAL		
d. FORMERLY RESTRICTED DATA			d. FABRICATE, MODIFY, OR STORE CLASSIFIED HARDWARE		
e. INTELLIGENCE INFORMATION			e. PERFORM SERVICES ONLY		
(1) Sensitive Compartmented Information (SCI)			f. HAVE ACCESS TO U.S. CLASSIFIED INFORMATION OUTSIDE THE U.S., PUERTO RICO, U.S. POSSESSIONS AND TRUST TERRITORIES		
(2) Non-SCI			g. BE AUTHORIZED TO USE THE SERVICES OF DEFENSE TECHNICAL INFORMATION CENTER (DTIC) OR OTHER SECONDARY DISTRIBUTION CENTER		
f. SPECIAL ACCESS INFORMATION			h. REQUIRE A COMSEC ACCOUNT		
g. NATO INFORMATION			i. HAVE TEMPEST REQUIREMENTS		
h. FOREIGN GOVERNMENT INFORMATION			j. HAVE OPERATIONS SECURITY (OPSEC) REQUIREMENTS		
i. LIMITED DISSEMINATION INFORMATION			k. BE AUTHORIZED TO USE THE DEFENSE COURIER SERVICE		
j. FOR OFFICIAL USE ONLY INFORMATION			l. OTHER *(Specify)*		
k. OTHER *(Specify)*					

DD FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE. Reset Adobe Professional 7.0

DD Form 254 (cont'd)

12. PUBLIC RELEASE. Any information *(classified or unclassified)* pertaining to this contract shall not be released for public dissemination except as provided by the Industrial Security Manual or unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release ☐ Direct ☐ Through *(Specify)*

to the Directorate for Freedom of Information and Security Review, Office of the Assistant Secretary of Defense (Public Affairs)* for review.
*In the case of non-DoD User Agencies, requests for disclosure shall be submitted to that agency.

13. SECURITY GUIDANCE. The security classification guidance needed for this classified effort is identified below. If any difficulty is encountered in applying this guidance or if any other contributing factor indicates a need for changes in this guidance, the contractor is authorized and encouraged to provide recommended changes; to challenge the guidance or the classification assigned to any information or material furnished or generated under this contract; and to submit any questions for interpretation of this guidance to the official identified below. Pending final decision, the information involved shall be handled and protected at the highest level of classification assigned or recommended. *(Fill in as appropriate for the classified effort. Attach, or forward under separate correspondence, any documents/guides/extracts referenced herein. Add additional pages as needed to provide complete guidance.)*

14. ADDITIONAL SECURITY REQUIREMENTS. Requirements, in addition to ISM requirements, are established for this contract. ☐ Yes ☐ No
(If Yes, identify the pertinent contractual clauses in the contract document itself, or provide an appropriate statement which identifies the additional requirements. Provide a copy of the requirements to the cognizant security office. Use Item 13 if additional space is needed.)

15. INSPECTIONS. Elements of this contract are outside the inspection responsibility of the cognizant security office. ☐ Yes ☐ No
(If Yes, explain and identify specific areas or elements carved out and the activity responsible for inspections. Use Item 13 if additional space is needed.)

16. CERTIFICATION AND SIGNATURE. Security requirements stated herein are complete and adequate for safeguarding the classified information to be released or generated under this classified effort. All questions shall be referred to the official named below.

a. TYPED NAME OF CERTIFYING OFFICIAL	b. TITLE	c. TELEPHONE *(Include Area Code)*

d. ADDRESS *(Include Zip Code)*	**17. REQUIRED DISTRIBUTION**
	☐ a. CONTRACTOR
	☐ b. SUBCONTRACTOR
	☐ c. COGNIZANT SECURITY OFFICE FOR PRIME AND SUBCONTRACTOR
e. SIGNATURE	☐ d. U.S. ACTIVITY RESPONSIBLE FOR OVERSEAS SECURITY ADMINISTRATION
	☐ e. ADMINISTRATIVE CONTRACTING OFFICER
	☐ f. OTHERS AS NECESSARY

DD FORM 254 (BACK), DEC 1999

Reset

Management Comments

Under Secretary of Defense for Intelligence

UNDER SECRETARY OF DEFENSE
5000 DEFENSE PENTAGON
WASHINGTON, DC 20301-5000

4 MAR 2014

INTELLIGENCE

MEMORANDUM FOR DEPUTY ASSISTANT INSPECTOR GENERAL FOR INTELLIGENCE EVALUATIONS AND SPECIAL PROGRAM ASSESSMENTS

SUBJECT: Response to DoD IG Draft Report, "Assessment of DoD Processes in Support of Committee on Foreign Investment in the United States (CFIUS) Determinations and Foreign Ownership, Control, or Influence (FOCI) Mitigation (Project No. D2012-DINT01-0159.000)"

In response to the February 10, 2014, request for comments on Office of the Inspector General Report D2012-DINT01-0159.000, we provide the attached response for the Under Secretary of Defense for Intelligence. We appreciate the opportunity to respond to your draft report. My point of contact is Ms. Valerie Heil at (703) 604-1112 or Valerie.L.Heil.civ@mail.mil.

Michael G. Vickers

Attachment:
As stated

cc:
Under Secretary of Defense for Acquisition, Technology and Logistics
Director, Defense Security Service

Under Secretary of Defense for Intelligence (cont'd)

RECOMMENDATION A: Issue guidance, in coordination with the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), that both delineates responsibility for coordination within respective services and organizations, and outlines a consistent process flow for National Interest Determinations to further a synchronized and coordinated approach to support Committee on Foreign Investment in the United States determinations and Foreign Ownership, Control or Influence mitigation.

- **USD(I) RESPONSE:** The Under Secretary of Defense for Intelligence (USD(I)) concurs with this recommendation. We have a proposed directive-type memorandum in the DoD policy issuance process that will meet the recommendation. Our goal is completion of the DoD policy issuance process with approval and publication of this DTM by the 3rd quarter of FY14.

RECOMMENDATION B1: Direct the creation of a centralized repository for cleared defense contracts, in coordination with USD(AT&L), to maintain DD Form 254s and other contract security requirements for classified contracts.

- **USD(I) RESPONSE:** USD(I) concurs as ongoing efforts by Defense Security Service (DSS) for the National Industrial Security Program (NISP) Contract Classification System (NCCS)) meet this recommendation. DSS began the planning and programming process for the NCCS, including collection of requirements from both government and industry stakeholders, in 2012. The DoD Investment Review Board (IRB) is now evaluating the NCCS. IRB approval is necessary before DSS can obligate any funds to build the NCCS. Funds are readily available under FY14 funding within DSS to support the project once IRB approval is received.

  DSS is also working with the Defense Procurement and Acquisition Policy Office within OUSD(AT&L) to determine the possibility of co-developing NCCS in order to reduce design and development lag time by leveraging an existing USD(AT&L) database.

  When completed, NCCS will serve as the single repository for contract security classification specifications to support DoD and the NISP. The expected NCCS initial operating capability is December 2015, with programmed enhancements beyond that date.

  In addition, the information collection for contract security classification specifications, represented by the DD Form 254 is tied to DoD's industrial security policy. OUSD(I) has the lead to garner approval of a revised DD Form 254, including coordination through the Office of Management and Budget's (OMB) interagency review, followed by a public comment period in the Federal Register with revision of DoD's industrial security policy. The OUSD(I) request for OMB approval of the revised DD Form 254 information collection will include data about the ongoing automation efforts to improve receipt and use of the contract security classification specifications. Our goal for OMB approval of a revised DD Form 254 information collection with DoD's updated industrial security policy is 2nd quarter of FY15.

Under Secretary of Defense for Intelligence (cont'd)

RECOMMENDATION B2: Designate DSS as executive agent for a centralized repository of cleared defense contracts in its role as the NISP Cognizant Security Office for DoD, 26 non-DoD agencies, and approximately 13,500 cleared contractors

- **USD(I) RESPONSE:** USD(I) does not concur with the recommendation for designation of an executive agent at this time as ongoing efforts by DSS do not require such an appointment. We will reevaluate whether there is a requirement for an executive agent, in coordination with OUSD(AT&L), during the development of the NCCS as well as the OMB/Federal Register information collection approval process.

Under Secretary of Defense for Acquisition, Technology, and Logistics

OFFICE OF THE UNDER SECRETARY OF DEFENSE
3000 DEFENSE PENTAGON
WASHINGTON, DC 20301-3000

ACTION MEMO

February 25, 2014

FOR: UNDER SECRETARY OF DEFENSE (AT&L)

FROM: Elana Broitman, DASD(MIBP)

SUBJECT: Partial Concurrence on DoD IG Report on the Assessment of DoD Processes in Support of CFIUS Determinations and FOCI Mitigation

- The Office of the DoD Inspector General (DoD IG) produced and released a February 2014 report (**TAB A**) on the assessment of DoD processes to support Committee on Foreign Investment in the United States (CFIUS) determinations and foreign ownership, control, or influence (FOCI) mitigation. This report responds to concerns raised by the U.S. Government Accountability Office and others.
- DoD IG concluded that extant policies clearly define requirements to support National Interest Determinations (NIDs), but that they do not effectively delineate roles and responsibilities to support the Services, agencies, and acquisition community, resulting in a significant decisions backlog.
- The following recommendations were made by the report:
    - RECOMMENDATION A: The Under Secretary of Defense for Intelligence (USD(I)) should issue guidance, in coordination with the Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)), that delineates responsibility for coordination within respective Services and organizations, and outlines a consistent process flow for NIDs to further a synchronized and coordinated approach to support CFIUS determinations and FOCI mitigation.
    - RECOMMENDATION B1: The USD(I) should direct the creation of a centralized repository for cleared defense contracts, in coordination with the USD(AT&L), to maintain DD Form 254s and other contract security requirements for classified contracts.
    - RECOMMENDATION B2: The Defense Security Service should be designated as the executive agent for a centralized repository of cleared defense contracts in its role as the National Industrial Security Program (NISP) Cognizant Security Office for DoD, 26 non-DoD agencies, and approximately 13,500 cleared contractors.
- USD(I) concurs with recommendations **A** and **B1**, but does not concur with recommendation **B2**. OUSD(I) argues that ongoing efforts do not presently require the designation of an

Under Secretary of Defense for Acquisition, Technology, and Logistics (cont'd)

executive agent. They assert that this requirement can be reevaluated, in coordination with OUSD(AT&L), during the development of the NISP Contracts Specification System as well as the OMB/Federal Register information collection approval process. USD(I)'s full responses are at **TAB B**.

RECOMMENDATION: **Partial Concurrence** on the DoD IG report by accepting recommendations **A** and **B1** and rejecting recommendation **B2**.

Approve: _____ Disapprove: _____

COORDINATION: TAB C MAR 2 8 2014

Attachments:
As stated.

Prepared by: Christian Marble, MIBP, 571-256-2975 (USA001114-14)

2

Acronyms and Abbreviations

CFIUS	Committee on Foreign Investment in the United States
COMSEC	Communications Security
DSS	Defense Security Service
e-FCL	Electronic Facility Clearance System
FINSA	Foreign Investment National Security Act
FOCI	Foreign Ownership Control or Influence
GAO	Government Accountability Office
GISWG	Government Industrial Security Working Group
MDA	Missile Defense Agency
MIBP	Manufacturing and Industrial Base Policy
NIDs	National Interest Determinations
NISP	National Industrial Security Program
NISPOM	National Industrial Security Program Operating Manual
ODNI	Office of the Director of National Intelligence
SF-328	Standard Form 328
SSA	Special Security Agreement
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(I)	Under Secretary of Defense for Intelligence


INSPECTOR GENERAL
INTEGRITY
EFFICIENCY
DEPARTMENT OF DEFENSE

Whistleblower Protection
U.S. Department of Defense

The Whistleblower Protection Enhancement Act of 2012 requires the Inspector General to designate a Whistleblower Protection Ombudsman to educate agency employees about prohibitions on retaliation, and rights and remedies against retaliation for protected disclosures. The designated ombudsman is the DoD Hotline Director. For more information on your rights and remedies against retaliation, visit www.dodig.mil/programs/whistleblower.

For more information about DoD IG reports or activities, please contact us:

Congressional Liaison
congressional@dodig.mil; 703.604.8324

Media Contact
public.affairs@dodig.mil; 703.604.8324

Monthly Update
dodigconnect-request@listserve.com

Reports Mailing List
dodig_report@listserve.com

Twitter
twitter.com/DoD_IG

DoD Hotline
dodig.mil/hotline

DEPARTMENT OF DEFENSE | INSPECTOR GENERAL

4800 Mark Center Drive
Alexandria, VA 22350-1500
www.dodig.mil
Defense Hotline 1.800.424.9098