wiley

The Defense Counterintelligence and Security Agency (DCSA) and Foreign Ownership, Control or Influence (FOCI) Handbook

wiley.law

TABLE OF CONTENTS

wiley

INTRODUCTION

The National Industrial Security Program (NISP) was established in 1993 by Executive Order 12829 to ensure that persons and entities with access to classified or sensitive information comply with industry safeguards equivalent to those within the U.S. government for protecting such information. Issued in accordance with the NISP, the National Industrial Security Program Operating Manual (NISPOM) sets forth the requirements, restrictions, and other safeguards to prevent the unauthorized disclosure of classified information. The NISPOM also prescribes procedures for the authorized disclosure of such information by the U.S. government to its contractors. The NISPOM is periodically updated to reflect changes and updates in industrial security matters.

U.S. government contracts that require access to classified information will not be awarded to companies operating under foreign ownership, control or influence (FOCI) unless adequate safeguards are in place to protect national security interests. U.S. contractors must take specific measures to mitigate or negate FOCI concerns in order to obtain and maintain classified contracts. The U.S. Department of Defense's (DOD) FOCI policy is premised, in part, on the notion that foreign investment in the U.S. defense industry serves national security interests and is encouraged; however, adequate safeguards must be in place to ensure that national security interests are protected.

Defense Counterintelligence and Security Agency (DCSA)

The DOD is fundamentally changing its approach to administering the NISP on behalf of all Executive branch departments and agencies. Through this initiative, the DOD is transitioning its security oversight approach from a schedule-driven compliance regime to an intelligence-based, threat-driven methodology.

Central to this reform is the Defense Counterintelligence and Security Agency (DCSA). Until June 2019, the Defense Security Service (DSS) served as the Cognizant Security Office for the DOD responsible for administering and implementing the NISP and regulatory control over classified information. On June 20, 2019, the DSS was renamed DCSA.

As a continuation of the former DSS, DCSA maintains industrial security responsibilities; however, the name change reflects DCSA's new role as administrator of personnel vetting and security clearance responsibilities for the entire federal government. Accordingly, federal security clearance entities are being merged into DCSA. The National Background Investigations Bureau (NBIB) was transferred from the U.S. Office of Personnel Management (OPM) to the DCSA on September 29, 2019. The DOD Consolidated Adjudications Facility (CAF)—which determines security clearance eligibility of non-intelligence agency DOD personnel occupying sensitive positions or requiring access to classified material—merged into DCSA on October 1, 2019. This consolidation of federal security clearance operations will be complete once the DCSA takes over certain functions of the Defense Information Systems Agency (DISA) and the Defense Manpower Data Center (DMDC), which are to be transferred to DCSA by October 1, 2020.

DCSA's current mission includes vetting and maintaining a trusted workforce, protecting critical technology, and providing professional security education. DCSA's primary functions are clearing industrial facilities, personnel, and

associated information systems; collecting, analyzing, and providing threat information to industry and government partners; managing FOCI in cleared industry; providing advice and oversight to industry; delivering security education and training; and providing information technology services that support the industrial security mission of the DOD and its partner agencies.

To carry out its NISP oversight duties, DCSA employs more than 350 industrial security representatives across 167 field offices in the United States. The field offices provide oversight and assistance to cleared industry. Currently, DCSA is responsible for providing security support services to approximately 13,000 cleared contractor facilities participating in the NISP.

Foreign Ownership, Control or Influence (FOCI)

DCSA grants security clearances that permit companies and their personnel to perform classified work. DCSA first clears the entity as a whole by issuing a Facility Security Clearance (FCL), and then clears its individual employees engaged in classified work by granting Personnel Security Clearances (PCLs). Key Management Personnel must have a PCL at the same level as the facility—Confidential, Secret, or Top Secret—before DCSA will issue a final FCL. In addition, a contractor operating under foreign ownership, control or influence must take certain steps to mitigate the FOCI before DCSA will issue an FCL.

A company is generally considered to be operating under FOCI whenever a foreign interest has the power, direct or indirect, to decide or direct matters affecting the company's operations, which may result in unauthorized access to classified information or adversely affect the performance of classified contracts. DCSA considers the following factors in the aggregate in evaluating whether a company is operating under FOCI and determining what mitigation measures are required:

- Record of economic and government espionage against U.S. targets by the foreign government;
- Company's record of enforcement or engagement in unauthorized technology transfer;
- Type and sensitivity of the information requiring protection;
- Nature and extent of FOCI by a foreign government;
- Company's record of compliance with U.S. laws, regulations, and contracts; and
- Nature of any bilateral and multilateral security and information exchange agreements.

To help inform DCSA's analysis of these factors, companies must complete the Standard Form (SF) 328, "Certificate Pertaining to Foreign Interest." The SF 328 includes the following questions, which assist DCSA in assessing the potential FOCI of a company:

- Do any foreign person(s), directly or indirectly, own or have beneficial ownership of 5% or more of the outstanding shares of any class of your organization's equity securities?
- Has any foreign person, directly or indirectly, subscribed 5% or more of your organization's total capital commitment?
- Does your organization, directly or indirectly through your subsidiaries and/or affiliates, own 10% or more of any foreign interest?
- Do any non-U.S. citizens serve as members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials?
- Do any foreign person(s) have the power, direct or indirect, to control the election, appointment or tenure of members of your organization's board of directors (or similar governing body) or other management positions of your organization, or have the power

to control or cause the direction of other decisions or activities of your organization?

- Does your organization have any contracts, agreements, understandings or arrangements with a foreign person(s)?
- Does your organization, whether as borrower, surety, guarantor or otherwise, have any indebtedness, liabilities or obligations to a foreign person(s)?
- During your last fiscal year, did your organization derive: (a) 5% or more of its total revenues or net income from any single foreign person? (b) In the aggregate, 30% or more of its revenues or net income from foreign persons?
- Is 10% or more of any class of your organization's voting securities held in "nominee" shares, in "street names" or in some other method which does not identify the beneficial owner?
- Do any of the members of your organization's board of directors (or similar governing body), officers, executive personnel, general partners, regents, trustees or senior management officials hold any positions with, or serve as consultants for, any foreign person(s)?
- Is there any other factor(s) that indicates or demonstrates a capability on the part of foreign persons to control or influence the operations or management of your organization?

A company must provide corporate documentation to clarify the nature and extent of the foreign interest for any "yes" answer to a question on the SF 328.

Importantly, a company's FOCI factors are not only reviewed as part of the initial facility clearance process, they are continuously revisited throughout the life of the FCL in order to address any changes that have occurred since the receipt of the clearance. For this reason, when a company with an FCL enters into negotiations for a proposed merger, acquisition, or takeover by a foreign entity, the cleared entity must notify DCSA and inform DCSA of the type of transactions under negotiation (stock purchase, asset purchase, etc.), the identity of the potential foreign investor, and plans to mitigate/negate FOCI.

FOCI MITIGATION INSTRUMENTS

DCSA has developed mechanisms for addressing issues that arise due to FOCI. The level of intrusiveness of the control structures (or mitigation instruments) has traditionally depended principally on the extent of FOCI and the sensitivity of the information underlying the classified contracts. In the event that foreign shareholders have the power to appoint one or more foreign nationals to the board, DCSA will likely require that the company take significant measures in order to remain eligible for classified contracts.

Foreign Ownership

The DCSA recognizes three general mitigation instruments to address FOCI of a company or corporate family: (1) a Board Resolution; (2) a Special Security Agreement/Security Control Agreement; and (3) a Voting Trust/Proxy Agreement, as well as some combination of the three instruments.

Board Resolutions

A Board Resolution is the least restrictive FOCI mitigation instrument. DCSA generally views this instrument as sufficient to mitigate FOCI where a foreign person does not own enough voting stock to elect a board member, or otherwise is not entitled to representation on the board of directors.

A Board Resolution identifies foreign shareholders and creditors, acknowledges the company's obligation to comply with all industrial security program requirements, and certifies that each of the foreign shareholders and creditors identified in the resolution will not have access to any classified information. This mitigation instrument is not available for companies that have foreign nationals serving on their boards of directors.

Security Agreements

The Special Security Agreement (SSA) includes significant industrial security measures within an institutionalized set of corporate practices and procedures. DCSA employs this mitigation instrument where a foreign person effectively owns or controls a company. Implementation of the SSA requires active involvement of senior management. It also requires that certain board members are U.S. citizens with no connection to the foreign interest (i.e., "Outside Directors"). The SSA maintains the foreign shareholder's right to be represented on the board of directors as an Inside Director with a direct voice in the management of the company, while denying the foreign shareholder unauthorized access to classified information. In addition, the SSA requires the creation of a Government Security Committee (GSC), which oversees classified and export-controlled matters for the company. Under an SSA, the GSC is composed of cleared officers/directors and Outside Directors.

Because the SSA is used when a company is effectively owned or controlled by the foreign entity, frequently, an SSA will involve the creation of a separate subsidiary to bid on and perform all classified work. This subsidiary must operate independently with respect to classified contracts and must demonstrate financial viability. The goal of an SSA is to create an arms-length relationship between the parent, which does not have access to classified information, and its cleared subsidiary. SSAs are formal arrangements that can be burdensome, as they give DCSA a prominent role in the management of the relevant company.

Although the SSA was not intended to permit access to information above the Secret Level, there are exceptions to this rule. Traditionally, a company operating under an SSA could access Top Secret or higher information only if it obtained a National Interest Determination (NID). In order to obtain a NID, a company is required to present "compelling evidence" that the release of the classified information "advances the national security interests of the United States." The NID process is currently undergoing major revisions as a result of long-standing concerns

by industry and recently enacted legislation. For example, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 eliminated the NID requirement effective October 1, 2020, for companies that are operating under FOCI and the parent company is within the National Technology and Industrial Base—which includes Australia, Canada, and the United Kingdom.

A Security Control Agreement (SCA) is used when a cleared company is not effectively owned or controlled by a foreign entity, but the foreign interest is nonetheless entitled to representation on the company's governing board. The SCA is substantially identical to the SSA with a few notable differences. Because the SCA is used when a company is not effectively owned or controlled by the foreign interest, the SCA imposes fewer restrictions on the company for the protection of classified information.

Companies operating under either an SSA or SCA must implement an approved Technology Control Plan (TCP). The TCP must establish "security measures determined necessary to reasonably foreclose the possibility of inadvertent access by non-U.S. citizen employees and visitors to information for which they are not authorized." In addition, the TCP must set forth measures designed to ensure "that access by non-U.S. citizens is strictly limited to only that specific information for which appropriate Federal Government disclosure authorization has been obtained[.]"

Companies operating under an SSA or SCA must also develop and implement an Electronic Communications Plan (ECP). The ECP must include adequate procedures for internet, email, phone use, etc., to ensure that no classified or export-controlled information is improperly disseminated through electronic communications. Importantly, companies/contractors operating under these agreements are subject to annual review and certification requirements.

Voting Trust Agreements and Proxy Agreements

Voting Trust Agreements (VTAs) and Proxy Agreements (PAs) are the most restrictive mitigation instruments. They are typically used to mitigate FOCI concerns where a foreign shareholder is in a position to control a U.S. company and the U.S. company is handling very sensitive information, usually at the Top Secret level. VTAs and PAs are substantially identical arrangements in which the voting rights of the foreign-owned stock are vested in Trustees (for VTAs) or Proxy Holders (for PAs), who are cleared U.S. citizens approved by DCSA.

Under such agreements, the company must establish that it is organized and financed in a manner that allows it to be a viable business entity that is entirely independent from the foreign shareholder. Accordingly, the Trustees and Proxy Holders act with all the prerogatives of stock ownership and have freedom to act independently from the foreign stockholders. Indeed, they are tasked with exercising management functions over the company in order to effectively insulate the company from the foreign stockholders. However, the Trustee or Proxy Holder may be required to obtain the approval of the foreign stockholder with respect to the following business activities: the sale or disposal of the corporation's assets or a substantial part thereof; pledges, mortgages or other encumbrances on the capital stock; corporate mergers, consolidations or reorganizations; the dissolution of the corporation; and the filing of a bankruptcy petition. Given that VTAs and PAs require foreign investors to relinquish control over the company, investors tend to disfavor these mitigation instruments.

As with the SSA and SCA, both the VTA and PA require the establishment of a GSC, which ensures that the company maintains and complies with policies and procedures to protect classified and export-controlled information.

Under a VTA and PA, the GSC is composed of Proxy Holders or Trustee Directors and those officers of the company who hold adequate security clearances. Further, both the VTA and PA require the establishment of a TCP and ECP. In addition, contractors operating under these agreements are subject to annual review and certification requirements.

In contrast to PAs, VTAs are rarely, if ever, employed as a FOCI mitigation mechanism.

Foreign Control or Influence

When foreign control or influence factors are present, but are unrelated to ownership, a mitigation plan must contain positive measures to effectively deny the foreign interest access to classified information and assure that the foreign interest cannot otherwise adversely affect the company's performance on classified contracts. For example, the DCSA has recognized the following measures:

- Adopting Special Board Resolutions;
- Assigning specific oversight duties and responsibilities to independent board members;
- Formulating special executive-level security committees to consider and oversee matters that affect the performance of classified contracts;
- Appointing a technology control officer;
- Modifying or terminating loan agreements, contracts, and other understandings with foreign interests;
- Diversifying or reducing foreign-source income;
- Demonstrating financial viability independent of foreign interests;
- Eliminating or resolving problem debt;
- Separating, physically or organizationally, the contractor component performing on classified contracts.

RISK-BASED SECURITY OVERSIGHT (RISO)

DCSA is changing the way the federal government conducts industrial security oversight of FCLs, including those under the FOCI mitigation instruments noted above. DCSA is working with industry to develop and implement a security methodology that couples NISPOM compliance with an oversight process that focuses on the particular assets at a cleared facility, the threats and vulnerabilities associated with those assets, and appropriate countermeasures. In doing so, the agency is changing the focus of its core functions from NISPOM compliance oversight, to a system that uses threat information to more accurately depict a facility's security posture by understanding the specific assets at a facility.

This fundamental change is a response the rise of foreign threats to the security of sensitive information and technology within U.S. industry. The rate of successful attacks on cleared facilities is unprecedented, and adversaries are using stolen information to upgrade their military capabilities and compete against the U.S. economy. DCSA is designing a NISP oversight methodology that evolves as threats evolve.

DCSA has acknowledged that its previous reliance on the NISPOM for oversight compliance proved to be insufficient in the modern threat environment. DCSA highlighted three drawbacks to the NISPOM's static nature: (1) failure to identify what information needs the most protection; (2) failure to respond to the evolving methods used by adversaries; and (3) failure to address inherent vulnerabilities in business processes and supply chains.

This new security review methodology was piloted as "DSS in Transition" (DiT) and is now called Risk-based Security Oversight (RISO).

The New Methodology

DCSA's RISO methodology is a fluid model that has evolved throughout its phased implementation rollout. DCSA has conceptualized RISO in five steps: Step 1: Prioritization; Step 2: Security Baseline; Step 3: Comprehensive Security Review; Step 4: Tailored Security Plan; and Step 5: Continuous Monitoring.

1. **Prioritization** of the new methodology rollout is conducted in two tiers. DCSA's initial prioritization occurs at the headquarters level and is based on technologies and programs deemed to be critical to national security. Secondary prioritization occurs at the field office level and is based on local workforce knowledge.
2. Contractors establish a **Security Baseline** by identifying national security assets at their facility and the security controls in place. The Security Baseline is then used to develop a Tailored Security Plan.
3. **Comprehensive Security Review** is an examination of business processes and security controls associated with asset lifecycles, supply chain protection, and related NISPOM compliance elements. Interviews with contractor subject matter experts are used to identify asset-focused vulnerabilities. Those vulnerabilities are then tracked through a Plan of Action & Milestone (POA&M) document and inform the development and implementation of an effective mitigation strategy.
4. Contractors and DCSA develop a **Tailored Security Plan (TSP)** based primarily on the Security Baseline and POA&M. Supplemental asset protection components may be included through an addendum.
5. DCSA will conduct **Continuous Monitoring** of TSPs through recurring reviews by contractors and DCSA personnel. The objective of Continuous Monitoring is to ensure that the TSP security controls adequately and effectively protect assets.

In 2017, DSS began monthly meetings with the National Industrial Security Program Policy Advisory Committee and industry representatives to develop this new security oversight methodology, and began running pilot exercises. Throughout 2018, DSS rolled out the RISO methodology at select facilities in four phases. In January through April 2018, DSS completed the first phase, which included four facilities. The second phase ran from July to September 2018 with eight participant facilities. The agency conducted the third phase in October 2018, and the fourth phase from November 2018 through January 2019. In 2019, the agency began implementing the DiT or RISO methodology at additional facilities, beginning with those holding priority technologies—assets and information most critical to national security. In June 2019, DSS became DCSA, and its RISO implementation rollout continues.

New Security Review & Rating Models

DCSA has introduced three security review types to serve as alternatives to the traditional Security Vulnerability Assessment (SVA) during the RISO transition: (1) Comprehensive Security Review (CSR); (2) Targeted Security Review (TSR); and (3) Enhanced SVAs.

CSRs follow the new RISO approach completely and are conceptualized as Step 3 of the new methodology. Facilities that undergo a CSR are not rated under the traditional rating model, and instead result in the development of a Tailored Security Plan. In 2018, field personnel conducted 61 CSRs and appear to have completed more than double that number in 2019.

TSRs follow the new methodology, except reviews are rated under the traditional ratings model and do not result in a Tailored Security Plan.

Enhanced SVAs initially introduced facility personnel to the RISO concepts of asset identification and mapping business processes related to asset protection. In 2019, DCSA began putting these concepts into practice by assisting contractors in identifying assets at their facilities, reviewing each facility's business processes related to security, and providing a matrix specific to the facility and technology used at the facility.

Enhanced SVAs are rated under the old rating model and closely follow the traditional security review format.

Under the traditional ratings process, the Vulnerability Assessment Rating Matrix, DCSA assigns all facilities a Starting Score of 700 points. Points are added to this score for NISP enhancements, which are actions a company takes to protect classified information that extend beyond what is required under the NISPOM. Following the 2016 NISPOM update, there were 10 NISP enhancement categories, including: information systems, active security organization membership, and physical security. Points are subtracted for violations based on NISPOM reference and not based on the number of violation occurrences. The traditional security ratings process accounts for both the size and complexity of a facility in arriving at the final security rating.

As part of the RISO rollout, DCSA conducted on-site security reviews at facilities selected through its internal prioritization process, and some facilities did not receive an on-site review. DCSA field offices engaged the contractors not receiving an enhanced review to assess the facility's security posture and discuss counterintelligence.

DCSA recently announced that it is developing a new industry rating model called the Security Rating Score (SRS). DCSA has engaged select industry partners to conduct dry runs and a limited pilot of the SRS; however, the agency has not yet made public the content of the SRS model or the implementation's details.

DCSA Engagement with Cleared Industry

As DCSA shifts its focus from NISPOM compliance to tailored critical technology protection, cleared industry must do the same. Contractors will need to identify critical assets at their facility and the security controls in place, document business processes and supply chains, and develop and monitor the effectiveness of Tailored Security Plans.

DCSA currently uses three engagement types as part of the RISO methodology: Targeted, Horizontal, and Vertical. Targeted engagement focuses on classes of critical technology at highest risk. Horizontal engagement focuses broadly on the business networks surrounding a classified contract, including end-to-end supply chain security. Vertical engagement has a programmatic focus from the government-client perspective and addresses the integrity of a given program across a team of contractors.

Comparing Old and New Approaches to Cleared Facility Oversight

Old Approach:

- Scheduling: Security reviews are scheduled on a 90-day plan, prioritizing facilities with FOCI mitigation agreements and those with classified information systems. Facilities with FOCI have security reviews 30 to 60 days before their mandatory annual meeting.
- Monitoring: Security reviews are focused on a contractor's compliance with NISPOM requirements and result in a security rating within the Vulnerability Assessment Rating Matrix.

New RISO Approach:

- Scheduling: DCSA security reviews are prioritized based on a facility's assets and threats to those assets as determined by national intelligence and the DOD's critical technologies and programs list. Contractors and government officials work together to identify assets at each facility and develop a Tailored Security Plan. Security reviews are scheduled in light of each facility's Tailored Security Plan.
- Monitoring: DCSA conducts a comprehensive security review to establish a Tailored Security Plan. Subsequent reviews assess the implementation and adequacy of the Tailored Security Plan. DCSA is currently developing a new rating system—the SRS—to complement the Tailored Security Plan.

OTHER RECENT DEVELOPMENTS

DCSA Granted Background Investigations Responsibility

Executive Order 13869, "Transferring Responsibility for Background Investigations to the Department of Defense," transferred the NBIB from OPM to DCSA, which was officially completed September 30, 2019. Congress initiated this transition in the National Defense Authorization Act for Fiscal Year (FY) 2018 in response to a major hack of OPM's personnel data.

SF 328 Revisions

SF 328, the Certificate Pertaining to Foreign Interests, has been revised twice since April 2017. Revisions to the form in April 2017 included removing the requirement for application of a corporate seal. In November 2018, revisions reflected the form's applicability to the DOD Enhanced Security Program and the DHS Classified Critical Infrastructure Protection Program, in addition to the NISP.

DCSA Growth

In an era of heightened national security concerns, DCSA and its FOCI oversight programs have grown significantly as illustrated in the RISO initiative. In addition, the transfer of the background investigations mission and personnel dramatically increases the size of DCSA. Congressional appropriations reflect DCSA's growth and transition expenses. For example, Congress allocated $545 million to DSS in FY 2015, $765 million for FY 2019, and $900 million for FY 2020.

To date, over 1 million industry personnel have been cleared, and approximately 10,000 companies and 13,000 contractor facilities are operating under NISP clearances. Further, there are approximately 268 FOCI mitigation agreements currently in effect and 674 FOCI facilities.

Congress expressed its interest in the successful transformation of the DCSA and DCSA's administration of security clearances in the National Defense Authorization Act for FY 2020 (NDAA 2020). NDAA 2020 was signed into law in December 2019 and directs the Director of DCSA to submit semiannual reports to the congressional defense committees on the processes in place for adjudicating security clearances and the progress made to address the backlog of security clearance applications. In addition, NDAA 2020 directs the Secretary of Defense to submit a report to Congress on the expanded purview of the DCSA.

Counterintelligence Report Finds Increased Attempts to Hack Sensitive/ Classified Information

The DCSA Counterintelligence Directorate issued its most recent "Targeting U.S. Technologies: A Report of Foreign Targeting of Cleared Industry" publication in February 2020. This unclassified report analyzes suspicious contact reports from cleared companies that DCSA received in FY 2018. DCSA also publishes an annual companion report at the classified level. Such annual reporting helps improve cleared industry's awareness of who instigated a hacking attempt, where it came from, the purpose of the attempt, and the method used. This information enables cleared companies to better identify and prevent future illicit contact.

In FY 2018, cleared industry filed approximately 50,000 reports of suspicious activities from cleared facilities operating within the NISP. DCSA classified 6,026 of these as suspicious contact reports (SCRs), which represents a 3% increase in SCRs from FY 2017. SCRs are reports of attempts by a foreign entity to obtain unauthorized access to sensitive or classified information and technology or compromise of a cleared employee. These attempts include actions by foreign governments and international terrorist organizations. In FY 2018, the most targeted technology was electronics, and integrated circuits were the most targeted category of electronics. Aeronautics systems were the second most targeted technology. Unmanned aerial vehicles were the

most targeted category of aeronautics systems, and unmanned or independent systems were commonly targeted across technology sectors. More than 40% of the SCRs identified East Asia and the Pacific as the source of the suspicious activity. The Near East was the second most common source of unauthorized collection attempts in FY 2018, as that region was associated with 13% of the suspicious contacts.

Foreign actors utilize a variety of methods to obtain sensitive or classified information and technology, but most frequently used the "attempted acquisition of technology" method. This method includes attempts to acquire protected information in the form of controlled technologies through front companies, third countries, or a direct purchase of firms. The second most common method of operation was request for information/solicitation, which involves directly or indirectly asking or eliciting personnel for protected information and technology.

In FY 2018, email was the method of contact foreign actors most commonly used to reach a target. The basic email method of contact includes unsolicited requests for information or purchase requests. The second most common method of contact in FY 2018 was also through email, but in the form of a phishing operation in which malicious content or attachments were embedded within the email for the purpose of compromising a network. Foreign actors are likely to continue to employ these methods of operation and contact in the future.

COMPLIANCE

Due Diligence

Contractors should be aware of the potential consequences of security breaches, including criminal prosecution of the corporation and/or responsible individuals; transfer of classified contracts to another contractor; revocation of the contractor's FCL; and/or suspension or debarment from all federal government contracts.

To prevent security violations, contractors should exercise due diligence to ensure that adequate safeguards are in place to protect classified and export-controlled information and take all necessary steps to promote maximum company-wide compliance with all policies and procedures concerning industrial security.

DCSA industrial security representatives are tasked with providing oversight and assistance to cleared contractor facilities and ensuring that U.S. classified information is protected. Accordingly, when in doubt regarding what is permitted under a given mitigation instrument, cleared or soon-to-be cleared contractors are strongly encouraged to consult with their industrial security representative.

Avoiding Potential Pitfalls

All cleared contractors are subject to DCSA inspection and review. Companies are also responsible for conducting internal reviews of their security systems to ensure the protection of classified information. DCSA has identified several violations that often result in poor security ratings. These include the following:

- Foreign parent management control
- Unauthorized co-location
- Shared services occurring without approval
- Inadequate ECP/TCP implementation
- Inadequate electronic communications monitoring
- Interlocking directors that were not disclosed or approved
- Insufficient IT network separation
- Disclosure of export-controlled information to the foreign parent without export authorization
- Failure to submit an Annual Compliance Report

- Failure to monitor/approve/document visits
- Insufficient implementation of the SSA, VTA, or PA
- Inadequate/failure to report (transfers of export material, communications, etc.)
- Unreported material changes
- Compensation committee consisting of only the Inside Director

Reporting and Investigating Security Breaches

The NISPOM requires that companies report security breaches promptly, stating that any "loss, compromise or suspected compromise of classified information, foreign or domestic, shall be reported[.] ... Classified material that cannot be located within a reasonable period of time shall be presumed to be lost until an investigation determines otherwise."

Specifically, a contractor must take the following steps to investigate and report a breach: (1) act "immediately" to "ascertain all of the circumstances surrounding" the breach; (2) if the "preliminary inquiry confirms a loss, compromise, or suspected compromise of any classified information occurred," an initial report is required, which states whether the security violation is a loss, compromise or suspected compromise, and identifies the surrounding circumstances; (3) investigate the suspected breach; and (4) submit a mandatory final report following the completion of the investigation, which must include all "material and relevant information" not provided by the initial report, identify the responsible individual(s), describe the corrective action taken, and present a determination regarding whether or not a breach occurred and the reasons for that conclusion.

WILEY'S FOCI AND DCSA OVERSIGHT EXPERIENCE

Wiley's International Trade Practice, recognized by *Chambers USA* as one of the country's elite international trade practices, regularly advises sophisticated industry clients on DCSA and FOCI matters. In addition to providing high-level legal analysis of potential FOCI issues, our attorneys provide step-by-step assistance with the DCSA clearance process. Ongoing counseling from our attorneys ensures that our clients remain in compliance with FOCI regulations in a dynamic international marketplace.

Wiley attorneys help clients navigate the policies and regulations governing the international economy, allowing us to provide comprehensive advice to FOCI clients in related fields. Our industry-leading export controls attorneys routinely help U.S. companies and foreign businesses with U.S. affiliates and subsidiaries to navigate the complex requirements of the International Traffic in Arms Regulations, the Export Administration Regulations, and economic sanctions administered by the Treasury Department's Office of Foreign Assets Control. We also have substantial experience assisting parties involved in foreign acquisitions, mergers, or takeovers in managing the Committee on Foreign Investment in the United States (CFIUS) review or investigation process, particularly transactions involving sophisticated technology or highly classified information.

Our FOCI experts collaborate with the firm's preeminent Government Contracts Practice to provide specialized advice to government contractors. Wiley is among the leaders in this area, consistently ranked by *Chambers USA* as one of only a few firms in the top tier of the nation's government contracts practices.

CONTACT US

Daniel B. Pickard
National Security Practice, Co-Chair
Partner
202.719.7285
DPickard@wiley.law

Tessa Capeloto
Of Counsel
202.719.7586
TCapeloto@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
NDaly@wiley.law

Richard C. Sofield
Partner
202.719.4500
RSofield@wiley.law

wiley.law