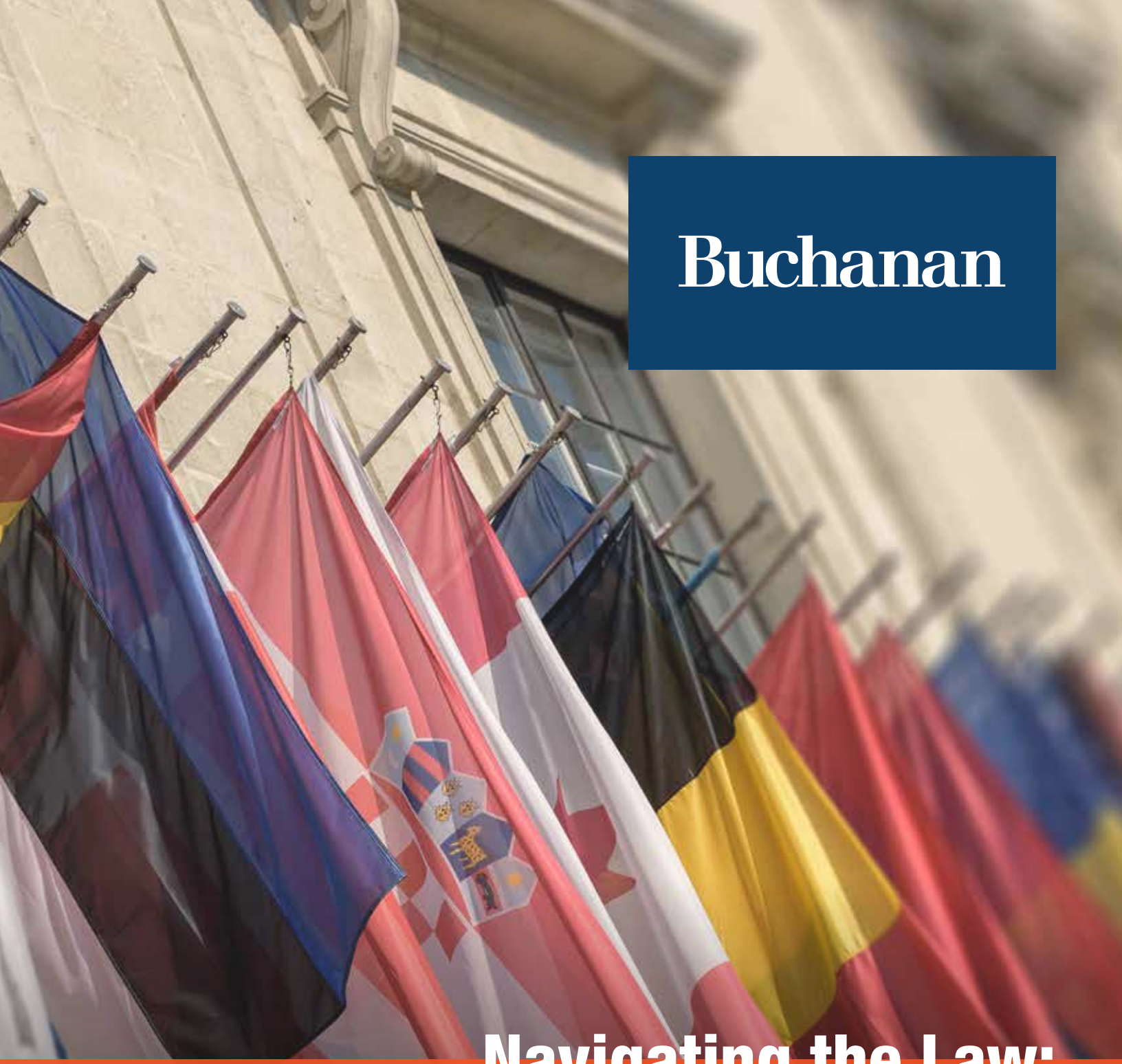


Buchanan

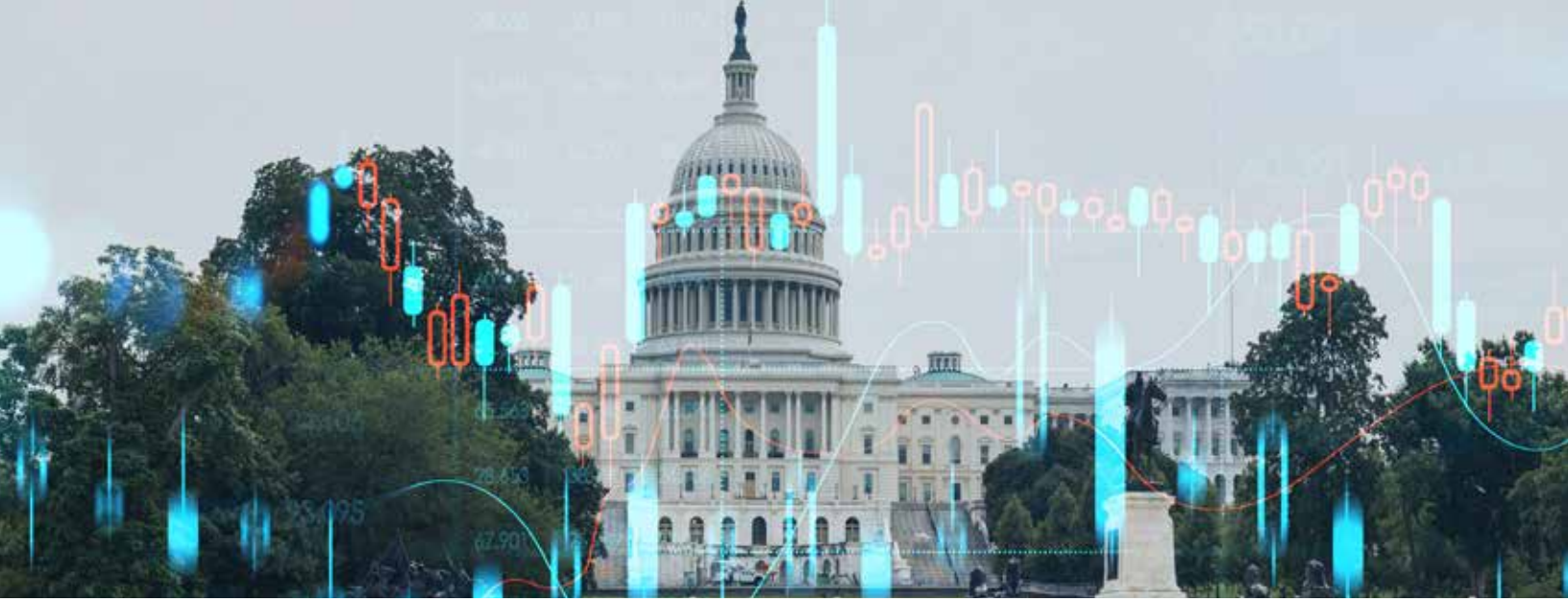
Navigating the Law:

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

Daniel B. Pickard, Shareholder, Chair,
International Trade & National Security Practice Group

September 2023

TABLE OF CONTENTS



This Defense Counterintelligence and Security Agency (DCSA) and Foreign Ownership, Control or Influence (FOCI) Handbook outlines the circumstances under which the DCSA grants security clearances that permit companies and their personnel to perform classified work. Items addressed in the handbook are FOCI mitigation instruments, the security review and rating process, and compliance, in addition to recent developments in FOCI enforcement.

INTRODUCTION

In 1993, President George W. Bush issued Executive Order 12829, which established the National Industrial Security Program (NISP) to protect classified information "released to contractors, licensees, and grantees of the United States Government." The executive order set standards for safeguarding sensitive and classified information while in the possession of industry partners. Additionally, the U.S. Department of Defense (DOD) is charged with overseeing and managing the NISP. The DOD has currently tasked the Defense Counterintelligence and Security Agency (DCSA) with implementing the NISP, including updating the National Industrial Security Program Operating Manual (NISPOM) periodically. The 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. In 2014, the Secretary of Defense added NISP regulations exclusive to foreign ownership, control, and influence (FOCI) at Title 32 of the Code of Federal Regulations at Part 117. The NISP regulations reflect the FOCI analysis and mitigation set out in NISPOM. However, the regulations standardize procedures and set timelines for certain events, notably for processing a National Interest Determination (NID). In 2020, the DOD revised the NISP regulations to include NISPOM itself.

U.S. government contracts involving classified information cannot not be awarded to companies operating with FOCI absent adequate safeguards to protect classified information. U.S. contractors must take specific measures to mitigate or negate FOCI concerns in order to obtain and maintain classified contracts. The DOD's FOCI policy is premised, in part, on the notion that foreign investment in the U.S. defense industry serves national security interests. However, adequate safeguards must be in place to ensure that national security interests, including classified information, are protected.

DEFENSE COUNTERINTELLIGENCE AND SECURITY AGENCY (DCSA)

The DOD is fundamentally changing its approach to administering the NISP on behalf of all U.S. Government departments and agencies. The DOD is transitioning its administration of industrial security oversight from a schedule compliance regime to an intelligence-based and threat-driven risk assessment methodology.

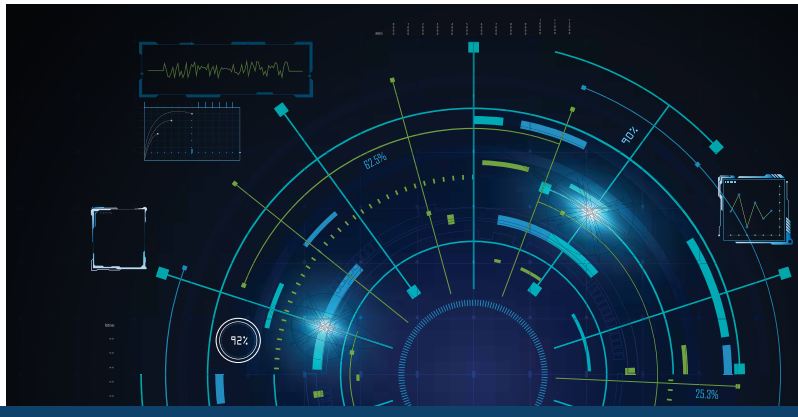
Central to this reform is the DCSA. Until June 2019, the Defense Security Service (DSS) served as the Cognizant Security Office for the DOD responsible for administering and implementing the NISP and regulatory control over classified information. On June 20, 2019, the DSS was renamed DCSA.

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. In October 2019, The National Background Investigations Bureau (NBIB) was transferred from the U.S. Office of Personnel Management (OPM) to the DCSA. Also in October 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. In October 2020, a second wave of consolidation occurred with certain functions of the Defense Information Systems Agency (DISA) and the Defense Manpower Data Center (DMDC), were transferred to DCSA, including the Personnel Vetting Transformation Office. In October 2021, the Defense Intelligence Agency transferred the National Center for Credibility Assessment (NCCA) to DCSA's Security Training Directorate.

At the same time, Section 847 of the National Defense Authorization Act for Fiscal Year 2020 expanded DCSA's oversight for FOCI. Section 847 requires expansion of existing NISP FOCI risk analysis to included companies not under NISP oversight but integral to the DOD supply chain. NISP policy also requires an expansion of DCSA's mission to include establishing a controlled unclassified information (CUI) program management office and may include further consolidation with other DOD entities.

DCSA's current mission includes vetting, industry engagement, education, and counterintelligence and insider threat support, secure the trustworthiness of the United States Government's workforce, the integrity of its cleared contractor support, and the uncompromised nature of its technologies, services, and supply chains. DCSA's primary functions are clearing industrial facilities, personnel, and information systems; collecting, analyzing, and providing threat information to industry and government partners; managing FOCI in the 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 over 12,000 government employees and contractor personnel operating from more than 160 regional and field offices in the United States. The field offices provide oversight and assistance to approximately 12,500 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 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. For a contractor to be eligible for an FCL, NISPOM states that they must (a) need access to the classified information in connection with a legitimate U.S. Government or foreign government requirement, (b) be organized and located in the United States, (c) have a record of integrity and lawful conduct in its business dealings, and (d) not be under foreign ownership, control, or influence to such a degree that a favorable entity eligibility determination for access to classified information would be inconsistent with the national interest.

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, directly or indirectly, to decide or direct matters affecting the company's management or operations. The concern is twofold, that the foreign interest's decisions may result in either 1) unauthorized access to classified information or 2) 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
- Record of enforcement and/or engagement in unauthorized technology transfer
- The type and sensitivity of the information that shall be accessed
- The source, nature and extent of FOCI
- Record of compliance with pertinent U.S. laws, regulations and contracts
- The nature of any pertinent bilateral and multilateral security and information exchange agreements
- Ownership or control, in whole or in part, by a foreign government.

To help inform DCSA's analysis of these factors, companies must complete Certificate Pertaining to Foreign Interests Standard Form 328 (SF 328) and provide supporting documentation. 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 your organization's securities held in "nominee shares," in "street names" or in some other method which does not disclose 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?

Importantly, a company's FOCI factors are not only reviewed as part of the initial facility clearance process, the factors are also continuously reviewed throughout the life of the FCL in order to address any changes 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 is required to notify DCSA of the type of transaction under negotiation (stock purchase, asset purchase, etc.), the identity of the potential foreign investor, plans to mitigate/negate FOCI, and copies of loan, purchase, and shareholder agreements, annual reports, bylaws, articles of incorporation, partnership agreements, other organizational documents, and reports filed with other U.S. government agencies.

REMEDIES AND MITIGATION OF FOCI

DCSA has developed several remedies to mitigate the risks 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.

The DCSA recognizes FOCI spans a spectrum from minor foreign influence to complete control depending on each company. DCSA primarily uses three 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 Proxy Agreement/Voting Trust as well as some combination of all three instruments. DCSA may also require mitigation through additional safeguard plans. For example, affiliated operations plans are used to restrict the sharing of certain business functions with affiliates of the company.

BOARD RESOLUTIONS

A Board Resolution is the least restrictive FOCI mitigation instrument. DCSA generally views Board Resolutions 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. Board Resolutions are not available for companies with foreign nationals serving as members of the board of directors.

SPECIAL SECURITY AGREEMENT AND SECURITY CONTROL AGREEMENTS

The Special Security Agreement (SSA) includes significant industrial security measures within an institutionalized set of corporate practices and procedures. DCSA employs SSAs where a foreign person effectively owns or controls a company. Implementation of the SSA requires active involvement and buy in by senior management. SSAs also require 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 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 solely 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 independently. The SSA subsidiary operates independently with respect to classified contracts and must demonstrate financial viability as a standalone business. The goal of an SSA is to create an arms-length relationship between the parent,

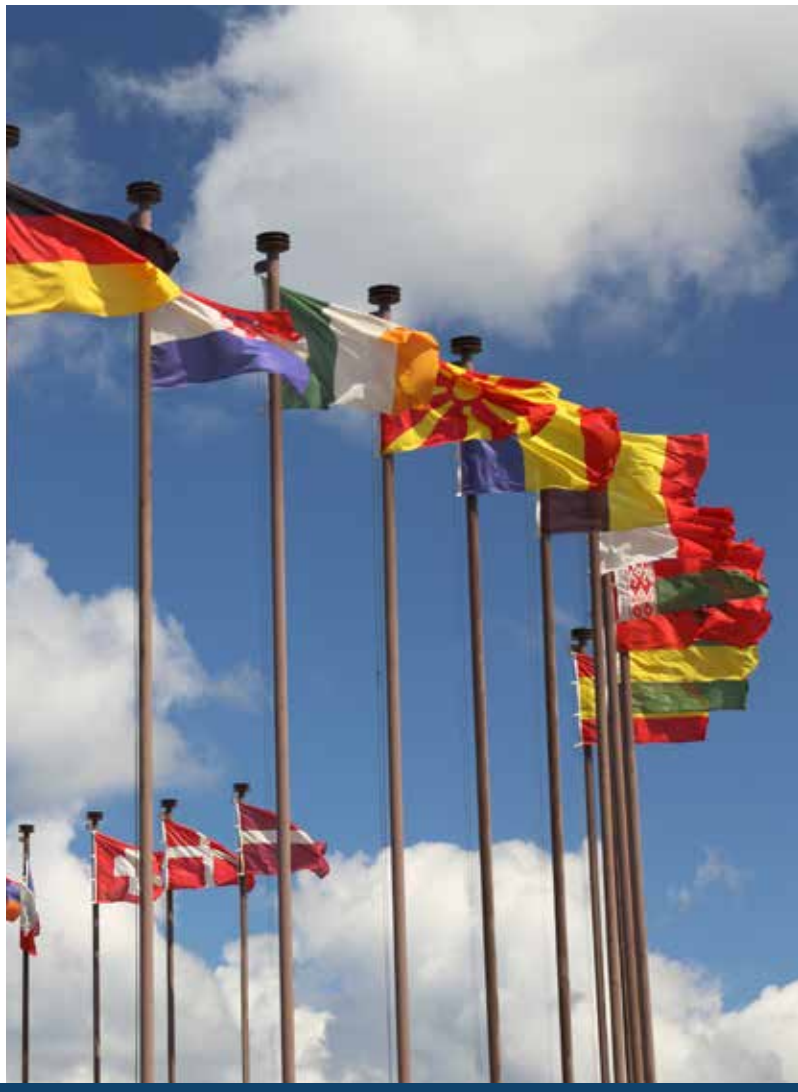
which does not have access to classified information, and its independent cleared SSA subsidiary. SSAs are formal arrangements that can be burdensome, as they give DCSA a prominent management role in the company.

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, as of October 2020, companies under FOCI with foreign interests within the National Technology and Industrial Base, which includes Australia, Canada, and the United Kingdom, no longer require a national interest determination.

DCSA uses a Security Control Agreement (SCA) when a cleared company is not effectively owned or controlled by a foreign entity, but the foreign interest does have representation on the company's governing board. An SCA is substantially identical to an SSA albeit 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 than an SSA.

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 prevent the possibility of 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 "access by non-U.S. citizens is strictly limited to only that specific information for which appropriate USG 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 to the foreign parent or its affiliates. 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 entirely independent from its foreign parent. Accordingly, the Trustees and Proxy Holders act with all the prerogatives of stock ownership and have freedom to act independently from the foreign parent company and its stockholders. Indeed, Trustee and Proxy Holders manage over the independent company in order to effectively insulate the company from the influence of foreign ownership.

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
- Creating special executive-level security committees to consider and oversee matters that affect the performance of classified contracts
- 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 INDUSTRIAL 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. Consequently, DCSA's industrial security oversight has shifted focus from compliance with NISPOM and direct foreign ownership to a risk-based assessment that gives more weight to different factors depending on the facility assets and circumstances of each company.

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 RiskBased Industrial Security Oversight (RISO).

THE NEW METHODOLOGY

DCSA's RISO methodology is a fluid model that has evolved overtime. 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. The Comprehensive Security Review has evolved in recent years to incorporate a supply chain risk management analysis and review of other indirect vulnerabilities.

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 conducts 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.

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.

Targeted Security Reviews 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 is developing a new industry rating model called the Security Rating Score (SRS) for maintaining an FCL. During the security review process, DCSA evaluates contractors in four security posture categories: NISPOM Implementation, Management Support, Security Awareness, and Security Community. DCSA provide a formal security rating of superior, commendable, satisfactory, marginal, or unsatisfactory that reflects the facility's effectiveness in protecting classified information.

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 and result in a SRS from DCSA.

COMPLIANCE DUE DILIGENCE

Contractors should be aware of the potential consequences of security breaches, including criminal prosecution 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 information and take all necessary steps to promote compliance with all industrial security policies and procedures, including export controls.

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 representatives.

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:

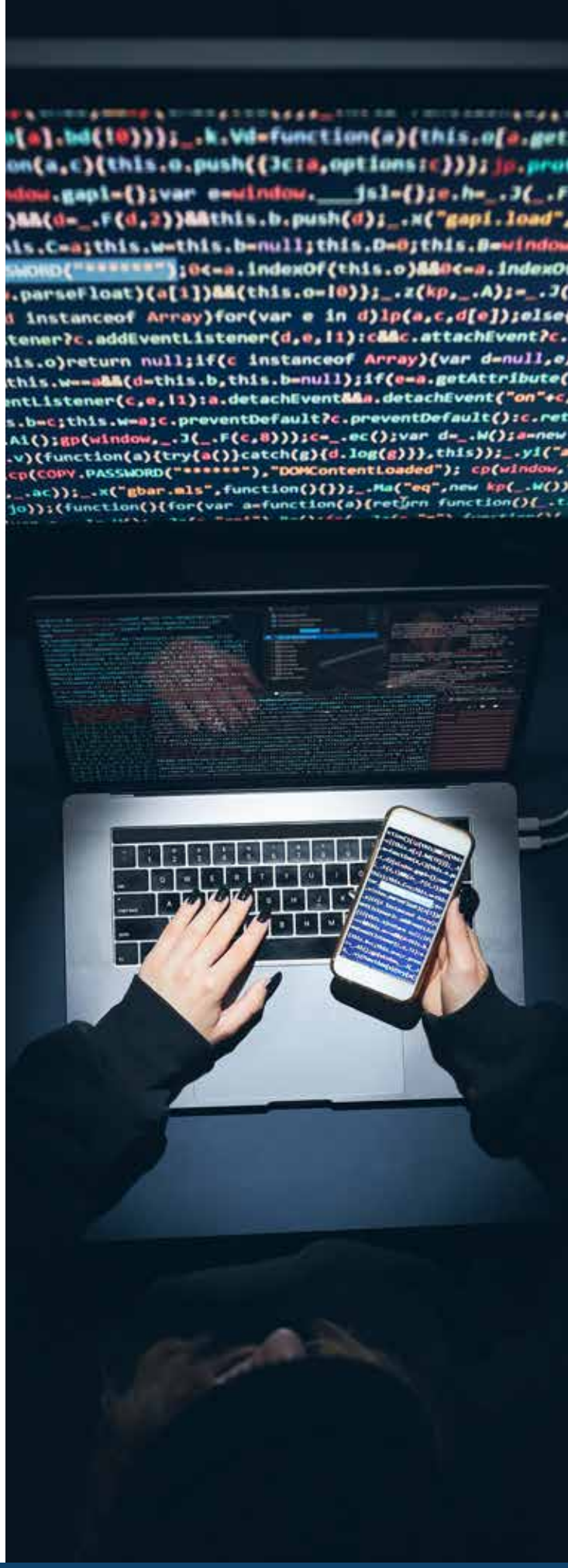
- Foreign parent management control
- Unauthorized co-location
- Shared services occurring without approval
- Inadequate ECP/TCP implementation
- Inadequate electronic communications monitoring
- Interlocking directors that were not disclosed or approved
- Insufficient IT network separation
- Disclosure 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 "the contractor will report any loss, compromise or suspected compromise of classified information." Further, "{a} ll cases in which it is known or there is reason to believe that classified information or material furnished or generated under the contract has been lost or disclosed to unauthorized persons will be reported promptly and fully."

Contractors 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 to DCSA (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.



BUCHANAN'S EXPERIENCE WITH FOCI

Buchanan Ingersoll and Rooney's team of national security attorneys has significant experience representing clients in the full range of issues before the Defense Counterintelligence and Security Agency (DCSA). Our attorneys have represented a wide range of companies with transactions subject to DCSA jurisdiction, from the due diligence phase to implementation to foreign ownership, control or influence (FOCI) mitigation measures.

Our International Trade & National Security practice group members have extensive experience working in government and agency capacities, as well as within industries we serve. We have fostered excellent working relationships with key federal, state, and regulatory bodies, and routinely represent clients on FOCI issues. Our well-rounded team is uniquely qualified to assist clients in navigating FOCI and ensuring compliance.

Daniel B. Pickard

Chair, International Trade & National Security Practice Group

Email: daniel.pickard@bipc.com
Phone: (202) 452-7936

Dan Pickard brings more than 20 years of experience providing guidance pertaining to mitigating Foreign Ownership, Control, or Influence (FOCI) issues and other national security issues. In cases of non-compliance and potential violations, Dan conducts internal investigations and represents clients before the relevant agencies in connection with investigations, voluntary self-disclosures, licensing, and enforcement actions. He has extensive experience in regard to foreign policy and national security matters such as U.S. economic sanctions, export controls, including the International Traffic in Arms Regulations (ITAR), anti-boycott measures, and the Foreign Corrupt Practices Act (FCPA). Dan provides comprehensive international trade law compliance guidance, including to U.S. and international clients that provide goods and services that may be regulated due to national security reasons. He develops customized and specialized corporate compliance programs related to the NISPOM, FCPA, ITAR, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Foreign Agents Registration Act (FARA).

Jordan A. Yeagley

Counsel

Email: jordan.yeagley@bipc.com
Phone: (717) 237-4822

Mert Ermen Arkan

Associate

Email: mert.arkan@bipc.com
Phone: (202) 452 7924

David B. Sessions

Associate

Email: david.sessions@bipc.com
Phone: (202) 452 7931

Claire M. Webster

Associate

Email: claire.webster@bipc.com
Phone: (202) 452-7934

Milton I. Koch, CPA

Strategic Consultant

Email: milton.koch@bipc.com
Phone: (202) 452-7937

Buchanan | WWW.BIPC.COM