

The Evolution of National Security in the U.S. and U.K.

Article By:

David Vance Lucas

Stephen Anderson

The U.S. and U.K. continue to adapt to global threats and shared national security risks

The U.S. and the U.K. are focused on common national security risks, including preventing foreign access to key emerging technologies, the integrity of the defense supply chain, protection of critical infrastructure, and advancements of research and development. There have been a series of announcements, rules, and regulations promulgated by U.S. and the U.K. the over the last year intended to better protect the common national security interests of both.

With a goal of “providing a point of view like no other,” members of Womble's Global Defense and Security Solutions Team have co-authored paired articles with a focus on specific changes in each jurisdiction, with this article providing the U.S. perspective. The U.K. corollary to this article is available [here](#).

Foreign Ownership Control and Influence

Defense contractors subject to Foreign Ownership Control and Influence (**FOCI**) pose a risk to national security. FOCI refers to a situation where a business engaged in providing products, services, or technology to the government is subject to potential control or influence by a foreign entity. More specifically:

- Foreign Ownership occurs when a foreign entity, whether a government, company, or individual, holds an ownership interest in a business, whether in the form of equity, debt, or other indicia of ownership.
- Foreign Control occurs when a foreign entity has the power to influence or direct the policies, operations, or decisions of a business, which can include minority ownership, voting rights, board representation, executive management, contractual agreements, or other arrangements that allow the foreign entity to dictate or alter the business's actions.
- Foreign Influence refers to situations where a foreign entity has the ability to affect the decisions or actions of a business through subjective, rather than direct control, via informal or indirect means, such as financial dependencies, strategic partnerships, or familial ties.

Defense contractors subject to FOCI pose a risk to national security due to the ability of foreign entities to exploit their ownership, control, or influence, to access, manipulate, or sabotage sensitive government projects, or protected locations.

Historically, U.S. FOCI mitigation has been limited to companies that hold U.S. Department of Defense (**DoD**) security clearances, have access to DoD classified or controlled but unclassified information (**CUI**), and have some level of non-U.S. involvement in their ownership, operations, or governance. U.S. defense contractors have been required to disclose foreign ownership by submitting a Standard Form 328 (**SF328**).

Defense industrial base supply chain integrity

Risks to the defense supply chain are asymmetric and can arise at any level in the supply chain – both at the prime and small business entity levels – as well as with classified and unclassified work. In May 2024, the DoD published a new DoD Instruction (**DoDI**) expanding the FOCI review process from contractors that hold DoD clearances and access classified information to all DoD contractors – cleared or not – that hold certain contracts in excess of \$5 million. [[*DoD Instruction 5205.87 “Mitigating Risks Related to Foreign Ownership, Control, or Influence \(FOCI\) for Covered DoD Contractors and Subcontractors”*](#)].

The May 2024 [*FOCI Instruction*](#) is the most recent effort by the DoD to expand protection to the defense supply chain. Regardless of clearance or access to classified information the May 2024 FOCI Instruction will subject certain DoD contractors to FOCI reviews and potential [*FOCI mitigation requirements*](#) by the Defense Counterintelligence and Security Agency (**DCSA**). The May 2024 FOCI Instruction expands FOCI reviews to a “covered contractor or subcontractor” that is “an existing or prospective contractor or subcontractor of the DoD on a contract, subcontract, or defense research assistance award (**DRAA**) with a value exceeding \$5 million”.

The DCSA is tasked to perform FOCI reviews for all “covered contractors” during the source selection process for covered contract. In general, DCSA FOCI reviews assess various FOCI risk factors to determine whether sufficient risk factors are present to warrant mitigation for a contract award. DCSA reviews can result in the implementation of a FOCI mitigation plan to protect national security from the FOCI security risk. FOCI mitigation plans vary from relatively simple corporate exclusionary resolutions and firewalls, to special purpose legal entities with independent directors and management, visitation, access, and communication restrictions, shared services and operations limitations, and other physical and electronic protections.

The FOCI Instruction does not specify the scope of the DCSA FOCI review for non-cleared DoD contractors. It is therefore currently unclear how FOCI risks will be mitigated for defense contractors that only perform unclassified contracts or only possess CUI. It is possible that the DCSA will establish new FOCI mitigation measures will be for unclassified or less sensitive contracts. The FOCI Instruction also potentially excludes contractors providing commercial products or services, so long as the subject contract is not determined to involve a “potential risk to national security or potential compromise of sensitive data, systems, or processes such as personally identifiable information, cybersecurity, or national security system.” The FOCI Instruction, however, does provide that DCSA, and “covered contractors” are required to execute and implement any required mitigation measures within 90 days after contract or DRAA award or commencement of performance on the contract.

The May FOCI Instruction also requires a “covered contractor” file and update a SF328 upon a change in beneficial ownership, which under existing regulations would apply to a 5% or more

change in the beneficial ownership of a “covered contractor.”

As a result, all DoD contractors and subcontractors, regardless of size and status of clearance, should carefully review the FOCI Instruction and understand its application to their business and their resulting compliance obligations. DoD contractors that do not currently hold a facility clearance but do have DoD contracts in excess of \$5 million should also familiarize themselves with the SF328 and establish policies and procedures to assess and comply with the FOCI Instruction and forthcoming Defense Federal Acquisition Regulation Supplement (**DFARS**) provision.

Continued expansion of U.S. Foreign Direct Investment regulations

Businesses involved in the U.S. defense industrial base have been historically protected from Foreign Direct Investment (**FDI**) by the Committee on Foreign Investment in the United States (**CFIUS**). The Foreign Investment Risk Review Modernization Act of 2018 (**FIRRMA**) expanded those historic protections to include certain Critical Technologies, Critical Infrastructure, and Sensitive Data – collectively referred to as covered “TID.” Notably, the U.K. is currently a “white-listed” allied country under FIRRMA, which lessens FDI scrutiny of U.K. investment in the U.S.

FIRRMA expanded CFIUS to address FDI impacting critical infrastructure and sensitive government installations. Part 802 of FIRRMA established CFIUS jurisdiction and review for certain covered real estate, including real estate in proximity to specified airports, maritime ports, military installations, and other critical infrastructure. Executive Order 14083 further expanded CFIUS coverage for certain agricultural related real estate. Covered installations are listed by name and location in appendixes to the CFIUS regulations. CFIUS recently added additional government installations to the proximity coverage of Part 802. The update captured substantially more covered real estate. Unlike covered Section 1758 technologies that can trigger a mandatory CFIUS filing, CFIUS jurisdiction for covered real estate currently remains only a voluntary filing.

FDI has been further complicated in the U.S. by the passage of individual U.S. State laws – often focused the acquisition of “agricultural land.” In the last two years, fifteen U.S. States enacted some form of FDI restrictions on real estate. Some States elected to incorporate U.S. Federal regulations regarding who is prohibited from acquiring certain real estate, while other States have focused on broadly protecting agricultural lands. State laws vary from those that prevent foreign ownership, to those that only require reporting foreign ownership.

Early diligence remains critical to any transaction in the United States that may result in foreign ownership or control of covered TID or real estate. Additional general information on U.S. CFIUS / FIRRMA is available on the [Treasury’s website](#).

Cooperation on Export Controls and Enforcement

A little over a year ago, the White House announced the “Atlantic Declaration” described as a “Twenty-First Century U.S.-U.K. Economic Partnership to ensure that our unique alliance is adapted, reinforced, and reimagined for the challenges of this moment.” The agreement includes provisions to improve export controls between the U.S. and its allies. In doing so, the U.S. also announced the intent to coordinate on the enforcement of export control regimes with the U.K., Australia, Canada, and New Zealand. The Atlantic Declaration is part of a long-term effort between the U.S. and its closest allies the “Five Eyes” - Australia, Canada, New Zealand, U.K., and U.S. – who have historically worked closely on common defense and intelligence matters.

The June 2023 announcement signalled a collaborative endeavour by the Five Eyes to enhance global security through coordinated enforcement of their respective export control regimes. While the specific details of the pact were not released, the announcement signalled that the countries were jointly committed to facilitating the exchange of information related to export control violations.

The U.S. Department of Commerce, Bureau of Industry and Security (**BIS**) also issued an announcement regarding coordination of enforcement by the Five Eyes in the areas of detentions, penalties, and diversions. The pact will permit will enable each of the countries to leverage their enforcement resources and capacities to prevent evasion and violation of export controls. The pact will also permit joint investigations and coordinated enforcement actions. The BIS announcement also noted an intent to strengthen global supply chains.

Proposed U.S. legislation will further modernize U.S. export control rules to make the flow of sensitive technology and services between the U.S., U.K. and Australia more efficient. Proposed measures have included designation of Five Eyes partners as “domestic sources” to allow Five Eyes partners to operate on a more equal footing with U.S. exporters and more targeted outbound controls on certain sensitive technologies. Proposed U.S. legislation would also provide the U.K. with an improved status under International Traffic in Arms Regulations. Doing so would help expedite trade in defense articles and research and development of controlled technologies. From a business perspective, if passed, new U.S. – U.K. export legislation may lessen licensing requirements and time delays for defense related sales, services and R&D between the U.S. and the U.K.

From an operational perspective, companies engaged in international trade should remain diligent in their export compliance efforts. From a compliance perspective they should be aware that an export control violation may result in investigative referrals or liability across multiple jurisdictions.

Womble Bond Dickinson U.K. Insight on the Approach in the U.K.

The approach taken to protecting national security in the U.K. has been changing, in part through a series of new laws that interpret national security as a broad concept.

The National Security Act 2023 might have national security as its title but, on the face of it, this could be seen as misleading since the Act applies in a much wider context.

The Procurement Act 2023 contains a national security exemption and a number of exclusions and rights linked to national security, but without defining what the term means.

Most recently, it was announced in the July 2024 King's Speech (which sets out the U.K. government's legislative agenda), that the new U.K. Labour Government will conduct a Strategic Defence Review to ensure that the U.K.'s defence capabilities are matched to the changing nature of global strategic threats.

In a corollary to this article, U.K. members of Womble's Global Defense and Security Solutions Team address how the concept of 'national security' is evolving in the U.K., and how the changes are impacting U.K. national security related legislation. You can find the related Womble' U.K. Defence and Security team U.K. article [here](#).

Copyright © 2025 Womble Bond Dickinson (US) LLP All Rights Reserved.

Source URL: <https://natlawreview.com/article/evolution-national-security-us-and-uk>