The Year in Review

Volume 53 International Legal Developments
Year in Review: 2018

January 2019

Aerospace and Defense Industries

Johny Chaklader
Michael Bealy
Neal Petro
Danish Hamid

Recommended Citation

This Industries is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in The Year in Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
Aerospace and Defense Industries

JOHNY CHAKLADER, MICHAEL BEALEY, NEAL PETRO, DANISH HAMID*

This article addresses some of the most significant legal and policy developments relevant to the aerospace and defense industries in 2018, including U.S. tariff actions against China, a new conventional arms policy, assessments on the manufacturing and defense industrial base and supply chain of the United States, the completion of a first full-scope, Defense Department financial statement audit, and key changes to national security reviews of foreign investments and acquisitions.

I. U.S. Tariff Actions Against China

Over the past year, the United States imposed additional tariffs on over two hundred billion dollars of imports from China. The following section outlines key developments associated with the ongoing U.S.-China Trade War.

On August 18, 2017, the U.S. Trade Representative (USTR) launched an investigation under Section 301 of the Trade Act of 1974.1 The USTR concluded that: (a) China uses joint venture requirements, foreign investment restrictions, and administrative review and licensing processes to require or pressure technology transfer from U.S. companies; (b) China deprives U.S. companies of the ability to set market-based terms in licensing and other technology-related negotiations; (c) China directs and unfairly facilitates the systematic investment in, and acquisition of, U.S. companies and assets to generate large-scale technology transfers; and (d) China conducts and supports cyber intrusions into U.S. commercial computer

* Johny Chaklader served as committee editor of this article, leads BDO USA, LLP’s Export Controls and International Trade practice, and is a Director in the firm’s Industry Specialty Services—Government Contracts group, where Michael Bealey is a Senior Associate and Neal Petro is an Associate. Johny Chaklader, Michael Bealey, and Neal Petro contributed to sections I through IV of this article. Danish Hamid is a partner at a prominent international law firm and is based in Washington, D.C. He has a comprehensive international corporate, regulatory, and investigations practice. Danish Hamid contributed section V of this article. The views expressed herein are solely those of the authors and not of their respective firms. This article is intended for informational purposes only and does not constitute legal advice.

1. Office of the President, Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation (Mar. 22, 2018).
networks to gain unauthorized access to commercially valuable business information.\(^2\)

As a result of these findings, the USTR imposed an additional 25% tariff on a “first tranche”—$34 billion worth—of imports from China that took effect on July 6, 2018. The U.S. then launched a 25% tariff hike on a “second tranche”—$16 billion worth—of imports from China that took effect on August 23, 2018. In response, the Chinese Ministry of Commerce issued a retaliatory tariff of 25% on $16 billion worth of U.S. imports. The U.S. responded with a 10% tariff hike on a “third tranche”—$200 billion worth—of Chinese imports that took effect on September 24, 2018, and announced a possible increase to 25% on another $267 billion worth of imports from China in January 2019.

USTR held public hearings and solicited public comments during each round of tariff hikes. USTR also opened dockets for companies to submit product exclusion requests for items covered under the first and second tranches. When evaluating product exclusion requests, USTR considered: (1) whether the product in question was available from non-Chinese sources; (2) whether the new Section 301 tariff would cause “severe economic harm” to the company; and (3) whether the product is strategically important or related to the “Made in China 2025” industrial policy. Thus far, USTR has granted very few requests for Harmonized Tariff Codes or products to be excluded from the additional duties.

These actions led to sharp cost increases for a wide swath of U.S. importers, manufacturers, and distributors, including those in the Aerospace and Defense industries. U.S. companies are reviewing their import strategies and exploring alternative supply lines where possible to mitigate the impact of new tariffs.

II. New Conventional Arms Policy (CAP)

During FY 2018, the United States-authorized arms-export market rose thirteen percent to $192.3 billion.\(^3\) This growth was accompanied by a renewed focus on better aligning the United States’ approach to conventional arms transfers with its national and economic security interests.

On April 19, 2018, President Trump issued a National Security Presidential Memorandum regarding the United States’ Conventional Arms Transfer Policy.\(^4\) The memorandum outlines a number of policy objectives for U.S. arms transfers including: (a) bolstering the security of the United States and its allies; (b) maintaining technological advantages of the United

---

States military; (c) increasing trade opportunities for United States companies; (d) strengthening the manufacturing and defense industrial base and lower unit costs for the United States and our allies and partners; (e) facilitating ally and partner efforts, through United States sales and security cooperation efforts; (f) strengthening relationships and enhancing military interoperability; (g) preventing proliferation by exercising restraint in transfers; (h) continuing participation in multilateral agreements to promote shared national policies of restraint; (i) working to assist other state suppliers of conventional arms in developing export control mechanisms; and (j) continuing to meet the requirements of all applicable statutes, including the Arms Export Control Act, the Foreign Assistance Act, the International Emergency Economic Powers Act, and the annual National Defense Authorization Acts.

The memorandum establishes that arms transfer approvals must account for a number of considerations, including the: (a) national security of the United States; (b) appropriateness of the transfer; (c) degree to which the transfer contributes to ally interoperability; (d) consistency with the United States’ interests in regional stability; (e) effect on the United States’ technological advantage; (f) recipient’s nonproliferation record; (g) transfer’s contribution to counter threats to national security; (h) economic security of the United States and its innovation; (i) transfer’s financial or economic effect on United States industry and effect on the defense industrial base; (j) recipient’s ability to obtain comparable systems from competing foreign suppliers; (k) likelihood that a transfer may undermine international peace and security, and (l) the United States’ actual knowledge at the time of authorization that the transferred arms will be used to commit human rights abuses.

In July 2018, the U.S. Secretary of State submitted an Implementation Plan required under the Conventional Arms Policy. The plan goals are to be implemented in three “Lines of Effort” (LOE). The first LOE prioritizes strategic and economic competition. This LOE tasks agencies with reorienting the U.S. to assume a proactive arms transfer approach and address challenges in increasing strategic competition. The second LOE calls upon agencies to streamline the International Traffic in Arms Regulations, revise the United States Munitions List, update the Commerce Control List, and establish objective milestones and standard timelines for Foreign Military Sales (FMS) transactions. The third LOE tasks agencies to create conducive environments by working with Congress and the business community to: (a) facilitate efficiency in defense trade; (b) improve the approach to developing FMS requirements; (c) reduce costs associated with FMS, and (d) improve efforts to promote trade.

5. U.S. Dep’t of State, Conventional Arms Transfer (CAT) Policy Implementation Plan Update (Nov. 8, 2018).
III. Review of Defense Industrial Base and Supply Chain

On July 21, 2017, President Trump issued Executive Order 13806 on assessing and strengthening the manufacturing and defense industrial base and supply chain of the United States. The order highlighted several issues with the defense industrial base including the loss of American factories, key companies, and manufacturing jobs. In addition, it required an assessment of the manufacturing capacity, defense industrial base, and supply chain resiliency of the United States to be delivered within 270 days of the order’s issuance.

On October 5, 2018, the Department of Defense (DOD) presented its report, “Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States” to President Trump. The report evaluated risk on current and planned operating priorities as of the late 2017 to early 2018. An Interagency Task Force led by the DOD developed sixteen working groups which included over 300 subject-matter experts across the government. Nine of the working groups focused on traditional sectors which included areas such as Aircraft, Ground Systems, and Shipbuilding while seven working groups assessed cross-cutting capabilities such as Cybersecurity for Manufacturing, Electronics, and the Workforce.

The working groups identified five macro forces that cause risk across the industrial base. These macro forces include: (a) sequestration and uncertainty of U.S. government spending; (b) decline of U.S. manufacturing capability and capacity; (c) U.S. government business practices; (d) industrial policies of competitor nations; and (e) diminishing U.S. Science Technology Engineering and Math trade and skills. The working groups categorized industry risk into the following archetypes: (a) sole source; (b) single source; (c) fragile supplier; (d) fragile market; (e) capacity constrained supply market; (f) foreign dependency; (g) diminishing manufacturing sources and material shortages; (g) gap in U.S.-based human capital; (h) erosion of U.S.-based infrastructure; and (i) product security.

The DOD identified several ongoing efforts to combat these challenges as well as recommendations for investment, policy, regulation, and legislation. In particular, the DOD advocates for an industrial policy that supports national security priorities, including the need to diversify from dependence on politically unstable supply sources. The DOD’s recommendations are organized into an Action Plan flowing from a comprehensive study on modernization efforts.

IV. Department of Defense Financial Statement Audit

On November 16, 2018, the Department of Defense announced it had completed its first full-scope, department-wide financial statement audit. The department began the audit in December 2017, which included more than 1,200 auditors and 900 site visits at over 600 locations. Five organizations from the department received a clean opinion, which indicates no discrepancies in their records. These organizations included the U.S. Army Corps of Engineers—Civil Works, Military Retirement Fund, Defense Health Agency—Contract Resource Management, Defense Contract Audit Agency, and the Defense Finance and Accounting Services Working Capital Fund. Two other organizations received a modified opinion including the Medicare-Eligible Retiree Health Care Fund and the Defense Commissary Agency. Other agencies within the department received disclaimers, which mean that issues were found with financial reporting, inventory discrepancies, and information technology systems security issues. Nonetheless, auditors noted that the Army, Navy, and Air Force properly accounted for major military equipment, and military and civilian pay. In addition, no evidence of fraud was found.

V. Significant Changes Impact National Security Reviews of Foreign Investments and Acquisitions in the Aerospace and Defense Industries

2018 has seen major legislative and regulatory developments regarding the Committee on Foreign Investment in the United States (CFIUS), the U.S. inter-governmental agency committee responsible for screening foreign investments in or acquisitions of U.S. businesses. On August 13, 2018, the President of the United States signed the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) into law. FIRRMA amends Section 721(a) of the Defense Production Act of 1950, the law which governs CFIUS. On October 10, 2018, the Department of the Treasury issued interim regulations (the Interim Regulations) pursuant to FIRRMA which, among other matters, require parties to certain types of investments or

---

11. 31 CFR § 800.101.
acquisitions of U.S. critical technology/defense companies to file mandatory declarations with CFIUS. In this context, critical technologies include items subject to various U.S. export controls as well as “emerging and foundational technologies” that have yet to be defined by future export control regulations issued pursuant to the Export Control Reform Act of 2018 (ECRA). ECRA contemplates that various government agencies (including those part of CFIUS) will coordinate efforts between themselves, and their respective processes will be interlinked, especially with respect to regulating critical technology. New export control regulations are expected. In this regard, on November 19, 2018, the Bureau of Industry and Security of the Department of Commerce (BIS) issued an Advance Notice of Proposed Rulemaking (the ANPRM) titled “Review of Controls for Certain Emerging Technologies.” The ANPRM seeks public comment on identifying “emerging technology” for export control purposes, which in turn will impact CFIUS’s jurisdiction.

A. OVERVIEW OF CFIUS

U.S. law authorizes CFIUS to review certain foreign investments in or acquisitions of U.S. businesses, otherwise known as “covered transactions.” CFIUS evaluates covered transactions to determine their effect on the national security of the United States. Based on this review, CFIUS advises the President of the United States. U.S. law authorizes the President to suspend or prohibit a covered transaction if, in the President’s judgment, there is credible evidence that the foreign investor or acquirer might take action that threatens to impair U.S. national security.

CFIUS has raised several concerns for both foreign investors and target companies. These concerns arose because CFIUS’s jurisdiction over foreign investments in the United States was already quite broad. With the introduction of FIRRMA, the scope of that jurisdiction has now expanded even further. CFIUS traditionally covered investments that resulted in

15. Specifically, FIRRMA defines “critical technologies” as (i) defense articles or defense services included on the U.S. Munitions List; (ii) items included on the Commerce Control List; (iii) certain nuclear facilities, equipment, parts, components, materials, software and technology prescribed by certain U.S. regulations; (iv) select agents and toxins covered by certain U.S. regulations; and (v) “emerging and foundational technologies” controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (to be identified by a regular, ongoing interagency process between CFIUS and the various U.S. export control agencies). Section 1703(a)(6)(A) of FIRRMA.
16. 31 CFR § 801.401.
17. Section 1703(a)(6)(A)(vi) of FIRRMA.
18. Section 1752(10) of ECRA.
20. 31 CFR § 800.207.
21. 31 CFR § 800.101.
foreign control of a U.S. business; now certain non-controlling investments are also covered by CFIUS.\textsuperscript{22}

A significant challenge for investors and companies is that the CFIUS review process can be opaque. CFIUS accounts for a variety of factors when determining the national security implications of a foreign investment. Although certain triggers can be identified by parties to an investment transaction in advance, CFIUS does not disclose all the specific data points that influence its determinations. CFIUS is counseled by U.S. national security agencies that may access non-public, classified information regarding the parties and the implications of the proposed investment which they will not share with the transaction parties.\textsuperscript{23}

B. Voluntary Notices to CFIUS

Applicable regulations permit parties to foreign investments and acquisitions to submit a voluntary notice to CFIUS explaining their respective backgrounds, the details of the proposed transactions, and the reasons why they feel that U.S. national security will not be impaired by the transaction.\textsuperscript{24} If the notice is compelling, CFIUS can inform the parties that it does not intend to take any further action, resulting in a safe harbor which would protect the foreign investment from further CFIUS challenges in the future.\textsuperscript{25} However, if CFIUS identifies a concern arising from the notice, CFIUS may launch an investigation, propose mitigation measures, and inform the parties that CFIUS will recommend that the President block the transaction unless the parties withdraw on their own accord.\textsuperscript{26}

CFIUS is not subject to any statute of limitations. Parties that fail to submit a voluntary notice with respect to a deal that poses material risk may be subject to CFIUS scrutiny and challenge at any time after the transaction closes. CFIUS may self-initiate a review and direct the parties to submit a notice to CFIUS six months, one year, five years, or at any other point after the transaction is completed. CFIUS may also question the parties as to why they did not submit a notice to CFIUS before completing their deal. If the parties are unable to provide a compelling explanation, CFIUS may view them with suspicion and apply a more aggressive scrutiny standard during its self-initiated review. Companies in the aerospace and defense industries traditionally have caused significant concern to CFIUS, especially if those companies maintain classified contracts with the U.S. government or

\textsuperscript{22} Section 1703(a)(4)(D) of FIRRMA.
\textsuperscript{23} The Director of National Intelligence serves as an ex officio member of CFIUS and provides independent analyses of any national security threats posed by transactions. The Foreign Investment and National Security Act of 2007, Public Law 110-49, 121 Sta. 246, which amends the DPA.
\textsuperscript{24} 31 CFR § 800.401.
\textsuperscript{25} 31 CFR § 800.601.
\textsuperscript{26} 31 CFR § 800.218, 800.503, 800.506, 800.507.
Parties to foreign investments in those industries should reveal their intentions to CFIUS in advance.

C. The Passage of FIRRMA

CFIUS has been in place for many years. For the first time in a decade, however, Congress decided on a non-partisan basis to update and enhance CFIUS’s role with the promulgation of FIRRMA. While FIRRMA does not expressly focus on investments from particular countries, Congressional commentary and debates regarding FIRRMA referenced Chinese-led investments as a motivating force behind FIRRMA. Also, FIRRMA itself states that when reviewing national security risks, CFIUS may consider, among various factors, whether the transaction involves a country of “special concern” that has a demonstrated or declared strategic goal of acquiring a type of critical technology or critical infrastructure that would affect U.S. leadership in national security areas. As has been well publicized, China has a declared strategic goal of acquiring critical technology.

D. Enhancements Introduced by FIRRMA

FIRRMA codifies certain practices that CFIUS had already been following. FIRRMA also introduces new elements that strengthen CFIUS’ ability to review foreign investments and acquisitions in the United States, especially concerning transactions targeting U.S. companies involved with critical technologies. Among various enhancements, FIRRMA (i) increases CFIUS’s budget; (ii) permits CFIUS to issue regulations allowing the committee to charge parties filing fees—not to exceed the lesser of 1% of the value of the transaction or $300,000 (adjusted for inflation); (iii) expands the types of corporate transactions that are subject to CFIUS’s jurisdiction; and (iv) requires the filing of mandatory declarations with CFIUS in certain limited circumstances subject to further regulation.

FIRRMA addresses most matters on a high-level basis and contemplates that

27. CFIUS is concerned with foreign investments in U.S. critical technology companies. Critical technologies include defense articles and defense services subject to U.S. export controls. 31 CFR § 800.209(a).
29. Section 1702 (c)(1) of FIRRMA.
30. FIRRMA defines “critical infrastructure” as (subject to further regulations prescribed by CFIUS) systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems or assets would have a debilitating impact on national security. Traditionally, critical infrastructures have included, but have not been limited to, electrical grids, telecommunications systems, transportation systems, and water supply networks. Section 1703 (a)(5) of FIRRMA.
31. Section 1723(2) of FIRRMA.
32. Section 1723(3) of FIRRMA.
33. Section 1703(a)(4) of FIRRMA.
34. Section 1706 of FIRRMA.
CFIUS and the U.S. Department of the Treasury will issue revised regulations to address those concerns on a more granular level. The Interim Regulations referenced above implement a pilot program concerning mandatory declarations impacting investments in certain types of critical technologies. CFIUS intends to use information gathered from this pilot program to design permanent regulations. The Treasury Department may implement additional pilot programs under FIRRMA to help guide its final regulatory regime.

E. CFIUS Jurisdiction Expanded

CFIUS has jurisdiction to review “covered transactions,” a term which traditionally included an investment, acquisition, merger, takeover, or joint venture that could result in the foreign “control” of a U.S. business. “Control” is the power—whether or not exercised—to directly or indirectly determine, direct, decide, take, reach, or cause decisions regarding important matters affecting a U.S. business. “Control” covers a majority investment as well as a dominant minority investment. CFIUS regulations hold that, in certain circumstances, a foreign person does not control a U.S. business (and can avoid CFIUS jurisdiction) if the foreign person holds 10% or less of the voting interest in the U.S. business and holds that interest solely for passive investment purposes. However, FIRRMA and the Interim Regulations have narrowed this passive investment exception for investments in certain types of critical technology companies. These recent developments suggest that there may be some cases where CFIUS can claim jurisdiction even if the investor has less than a 10% voting interest. For example, CFIUS jurisdiction may exist if a minority foreign investor gains access to material non-public information regarding critical technology.

FIRRMA expands CFIUS’s jurisdiction by adding the following matters to the scope of “covered transactions”: (i) certain types of real estate transactions; (ii) any “other investment” (discussed below) by a foreign person in any U.S. business that is involved with critical infrastructure, critical technology, or sensitive personal data; (iii) certain changes in a foreign investor’s existing rights with respect to a U.S. business if that change could result in foreign control of the U.S. business or an “other

35. 31 CFR § 801(II).
36. 31 CFR § 800.207, 800.224.
37. 31 CFR § 800.204.
38. 31 CFR § 800.204.
39. 31 CFR § 800.223, 800.302(b).
40. 31 CFR §§ 801.208, 801.302.
41. According to FIRRMA, CFIUS jurisdiction will cover the purchase, lease, or concession by or to a foreign person of certain real estate in close proximity (a distance within which the transaction could pose a national security risk) to U.S. military or other sensitive national security facilities. Sections 1703(a)(4)(B)(ii) and 1703(a)(4)(C)(ii) of FIRRMA.
investment”; and (iv) any other transaction or agreement designed to circumvent or evade CFIUS.42

Under FIRRM, “other investments” afford a foreign person the following abilities with respect to a U.S. business involved with critical infrastructure, critical technologies, or sensitive personal data of U.S. citizens: (i) access to any material non-public technical information in the possession of the U.S. business; (ii) membership or observer rights on the board of directors or equivalent governing body of the U.S. business; (iii) the right to nominate an individual to a position on the board of directors or equivalent governing body of the U.S. business; or (iv) any involvement, other than through voting of shares, in substantive decision making of the U.S. business regarding critical infrastructure, critical technologies, or sensitive personal data of U.S. citizens.44

F. MANDATORY DECLARATIONS TO CFIUS

One of the most significant features of FIRRM is that it introduces the concept of a mandatory declaration in certain circumstances. Parties that fail to file the mandatory notice with CFIUS, if applicable, may be subject to a fine up to the value of the investment.45

A declaration is supposed to be shorter than a formal notice and is not supposed to exceed five pages. FIRRM does not specify all the instances in which the parties must file a mandatory declaration; instead, FIRRM requires CFIUS to prescribe regulations specifying the types of covered transactions for which parties must file a mandatory declaration with CFIUS. CFIUS has yet to issue those regulations.46 However, CFIUS released the Interim Regulations that impose a pilot program that requires parties to submit a mandatory declaration concerning certain foreign investments in U.S. businesses that produce, design, test, manufacture, fabricate, or develop critical technologies in one of 27 industries identified by their NAICS code.47

42. Section 1703(a)(4) of FIRRM.
43. FIRRM defines “material non-public technical information” to mean information that (i) provides knowledge, know-how, or understanding, not available in the public domain, of the design, location, or operation of critical infrastructure; or (ii) is not available in the public domain, and is necessary to design, fabricate, develop, test, produce, or manufacture critical technologies, including processes, techniques, or methods. FIRRM also states that its definition of “material non-public technical information,” is subject to regulations prescribed by CFIUS. CFIUS has yet to issue revised regulations that will address this matter. As a result, further refinement with respect to this term is likely and it would be prudent to revisit the concept of “material non-public technical information” once CFIUS issues new regulations. Section 1703 (a)(4)(D)(ii) of FIRRM.
44. Section 1703 (a)(4)(D) of FIRRM.
45. Section 1706 of FIRRM.
46. Id.
47. 31 CFR 801.302, Annex A to Part 801 – Industries.
Those 27 industries include, but are not limited to: (i) Aircraft Manufacturing (NAICS Code: 336411); (ii) Aircraft Engine and Engine Parts Manufacturing (NAICS Code: 336412); (iii) Guided Missile and Space Vehicle Manufacturing (NAICS Code: 336414); (iv) Guided Missile and Space Vehicle Propulsion Unit and Propulsion Unit Parts Manufacturing (NAICS Code: 336415); (v) Military Armored Vehicle, Tank, and Tank Component Manufacturing (NAICS Code: 336992); (vi) Computer Storage Device Manufacturing (NAICS Code: 334112); (vii) Electronic Computer Manufacturing (NAICS Code: 334111); (viii) Optical Instrument and Lens Manufacturing (NAICS Code: 333314); (ix) Other Guided Missile and Space Vehicle Parts and Auxiliary Equipment Manufacturing (NAICS Code: 336419); (x) Radio and Television Broadcasting and Wireless Communications Equipment Manufacturing (NAICS Code: 334220); (xi) Search, Detection, Navigation, Guidance, Aeronautical, and Nautical System and Instrument Manufacturing (NAICS Code: 334511); and (xii) Semiconductor and Related Device Manufacturing (NAICS Code: 334413).48

The pilot program covers controlling as well as certain non-controlling investments that afford a foreign investor: (i) access to any material nonpublic technical information; (ii) membership, observer, or nomination rights on the board of directors; and (iii) any involvement in substantive decision-making regarding the critical technology (other than through voting shares).49 Even a 2% investment in a critical technology business in one of the designated industries can trigger a CFIUS mandatory declaration if any one of the conditions listed above are satisfied.

Once CFIUS has received a mandatory declaration, CFIUS has the ability to (i) request that the parties submit a written notice; (ii) inform the parties that CFIUS is not able to complete its review and the parties may file a written notice; (iii) initiate a unilateral review; or (iv) notify the parties that it has concluded all action.50 Even if the parties undergo the effort to file a mandatory declaration, they may still need to file a more substantial notice. In practice, certain parties may determine that their facts and circumstances merit filing a more detailed notice instead of the declaration. In addition, CFIUS’s approval of a transaction disclosed in a notice will result in a safe harbor protection (occasionally subject to certain conditions) that would apply not only to the foreign investor’s current investment covered by the notice, but also future investments by the same investor in the same company.51 In contrast, any safe harbor associated with CFIUS’s approval or no-action determination in relation to a declaration would be limited to the four corners of the current investment discussed in the declaration. CFIUS
would still retain jurisdiction over future investments by that foreign investor in the same company.

G. CFIUS AND EXPORT CONTROLS

A prior version of FIRRMA contemplated allowing CFIUS to claim jurisdiction in certain cases over a U.S. critical technology company's outbound transfers and contributions (including via a joint venture) of intellectual property to a foreign person, even if that transfer or contribution did not result in a foreign person gaining “control” over the U.S. business. This provision could have been a truly novel development that would have had a direct impact on a critical technology company seeking to assign or license its IP or associated support to a foreign joint venture or affiliate. However, the final version of FIRRMA did not expand CFIUS' jurisdiction over transfers and contributions of IP. Instead, Congress decided that it would be more appropriate for outbound contributions of IP to continue to be monitored under U.S. export control laws and not CFIUS. However, Congress determined that existing U.S. export controls were not sufficient to address these concerns. As a result, in parallel with FIRRMA, Congress also passed the Export Control Reform Act of 2018 (ECRA) to enhance export controls.

Although CFIUS will not regulate contributions of critical technology IP to foreign persons outside of covered transactions, from a practical perspective, the CFIUS process will continue to be connected closely to export control concerns. If a foreign person invests in or acquires a U.S. business that manufactures or develops products subject to export restrictions, CFIUS will consider this factor in its national security risk assessment of the transaction.52

H. ECRA AND THE ANPRM

ECRA contemplates that the Executive Branch of the U.S. government will reform and enhance U.S. export controls to address and restrict the transfer and contribution of certain types of critical technologies to foreign persons. FIRRMA itself expanded the definition of critical technologies to include “emerging and foundational technologies” that will be subject to export controls issued pursuant to ECRA.53 In an effort to help guide the ECRA regulatory process, BIS issued the November 19 ANPRM requesting public comment on identifying “emerging technologies” not already subject to export controls but that are essential to U.S. national security, including those that could provide the United States with qualitative military or intelligence benefits. The ANPRM lists 14 representative general categories of emerging technologies including, but not limited to, certain types of artificial intelligence, position, navigation, and timing technology, advanced

---

52. 31 CFR § 800.402(e)(4)(i).
53. Section 1703(a)(vi)(A)(vi) of FIRRMA.
computing technology, data analytics technology, logistics technology, robotics, hypersonics (flight control algorithms, propulsion technologies, thermal protection systems, or specialized materials for structures or sensors), and advance surveillance technologies. BIS has also indicated that it is still reviewing other emerging and cutting-edge technologies for proposed regulation.54

BIS required that the public deliver their comments in response to the ANPRM by December 19, 2018. Those comments may include, among other matters, suggestions on the definition of emerging technology, the criteria used for determining whether technologies are critical to U.S. national security, and the impact that such items would have on U.S. technological leadership. After receiving those comments, BIS will propose new export control rules governing emerging technologies and, which in turn, will trigger the CFIUS mandatory declaration in certain circumstances. BIS also intends to issue a separate ANPRM for “foundational technology” which will follow a similar process and impact the scope of the CFIUS mandatory declaration.55

55. Id.