Written Testimony of

Jonathan (Josh) S. Kallmer
Senior Vice President for Global Policy
Information Technology Industry Council (ITI)

U.S. House of Representatives
Committee on Financial Services
Subcommittee on Monetary Policy and Trade

H.R. 4311, the Foreign Investment Risk Review Modernization Act of 2017

April 12, 2018

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

United States House of Representatives
Committee on Financial Services
Subcommittee on Monetary Policy and Trade

H.R. 4311, the Foreign Investment Risk Review Modernization Act of 2017

Opening Remarks of Jonathan (Josh) S. Kallmer
Senior Vice President for Global Policy, Information Technology Industry Council (ITI)
Former Deputy Assistant U.S. Trade Representative for Investment (2007-2012)

April 12, 2018

Chairman Barr, Ranking Member Moore, members of the Subcommittee, thank you for your invitation to appear before this distinguished panel to discuss H.R. 4311, the Foreign Investment Risk Review Modernization Act (FIRRMA) of 2017.

My name is Josh Kallmer, and I am Senior Vice President for Global Policy at the Information Technology Industry Council, or ITI. ITI is a collection of 63 of the world's most innovative companies, representing every part of the technology sector – including hardware, software, services, and Internet – as well as companies from other sectors that depend deeply on information technology. Despite their diversity, all of our companies share a single goal, which is to bring about policy environments that enable innovation and maximize all of the benefits that technology provides, including economic growth, job creation, and tools for solving the world's most pressing challenges.

My perspectives on this subject also flow from my time in government. From 2007 to 2012, I served as Deputy Assistant U.S. Trade Representative for Investment. In that role I was

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org

responsible for developing and implementing U.S. international investment policy, served as lead U.S. negotiator for several investment treaties, and represented the Office of the U.S. Trade Representative (USTR) on the Committee on Foreign Investment in the United States (CFIUS). In five years sitting on CFIUS I participated in the review of hundreds of transactions and regularly represented USTR at political-level interagency meetings concerning transactions with particularly sensitive national security implications. I was also deeply involved in the process of drafting regulations during the last modernization of the CFIUS framework in 2007 and 2008.

On the basis of these professional experiences, as well as more than a decade as an international trade attorney in both private practice and government, I look forward to engaging today with the subcommittee and my fellow witnesses to discuss the important role that this legislation might play in addressing new and emerging types of security risks and in advancing U.S. national security overall. In particular, I would like to make three main points.

First, the national security concerns are real and legitimate, and FIRRMA can be an important part of a U.S. government strategy to address those concerns.

The United States has benefitted greatly from its longstanding openness to foreign investment. In 2015, U.S. affiliates of companies headquartered outside the United States employed 6.8 million Americans and paid those workers almost 25 percent more than the U.S. private sector average.[1] During the same year, some 70 percent of foreign investment inflows

[1] *See* "Foreign Direct Investment in the United States," *U.S. Department of Commerce*, Oct. 3, 2017, at 2.

went to the U.S. manufacturing sector,[2] and between 2010 and 2014 U.S. affiliates of non-U.S. companies created two thirds of the United States' 656,000 new manufacturing jobs.[3] Foreign investment contributes significantly – and frequently disproportionately – to U.S. employment, compensation, exports, and R&D spending, and it is in the national interest to maintain an open investment environment.

At the same time, the U.S. government has no more solemn and important responsibility than to protect the nation's security, and the United States should pursue its commitment to open investment consistent with that imperative. Our organization and the companies we represent respect and agree with the underlying national security objectives of this legislation. We are committed to working with Congress, the Executive Branch, and the entire stakeholder community to achieve these objectives.

We also agree that the proponents of FIRRMA have identified a compelling set of emerging national security risks that demand immediate and effective attention by the U.S. government. The world has changed dramatically since the last reform of the CFIUS legal framework a decade ago. Global business arrangements are more complex and diffuse. International business increasingly depends on the instant, cross-border movement of digital information. Transformational technologies are emerging at an accelerating rate, and the

---

[2] *See ibid.*

[3] *See* L. Wroughton and H. Schneider, "'Bad' foreign firms drive U.S. manufacturing jobs revival," *Reuters*, Jun. 30, 2017.

security implications of these new technologies are both more significant and more difficult to anticipate. And other countries are working harder than ever to use, exploit, and otherwise take advantage of these technologies to advance their own strategic, security, and economic interests.

FIRRMA contains a number of innovations that would improve the operation of the CFIUS process and enhance U.S. national security. We welcome, for example, the bill's proposed reforms to: (a) enable CFIUS to review certain real estate transactions in the proximity of military facilities; (b) prevent parties from using overly complex or opaque business arrangements to avoid CFIUS review; (c) require the submission of a declaration in situations involving significant foreign government interests; (d) expand the illustrative list of national security factors that CFIUS may consider in evaluating transactions; (e) clarify the role and elements of a CFIUS "risk-based analysis;" (f) improve monitoring of, and compliance with, mitigation agreements; and (g) ensure the availability of funding for CFIUS to function as intended.

Second, there are valid differences among views on how best to address the national security risks associated with "emerging critical technologies."

While I believe that we all agree on the desired destination of this debate – to strengthen U.S. national security in an increasingly complex world with ever more pressing security risks – it is clear there are meaningful disagreements on how we travel to that destination. These disagreements are healthy. Given the complexity of the issues at play, it is critical that we solicit a range of views from experts on security, technology, intelligence, and trade and investment policy to thoughtfully debate these matters in an open setting. Doing so increases the likelihood

that we will reach the best national security result for the country, while enabling the U.S. economy and American workers to realize the many benefits of foreign investment.

We offer our views on possible improvements to the bill in this spirit of open and thoughtful debate. In particular, our principal departure from the proponents of the bill on the best way to address these emerging national security risks relates to the proposed expansion of CFIUS jurisdiction under FIRRMA to cover outbound transfers of U.S. intellectual property to foreign persons. Our concerns relate primarily to Section 3(a)(5)(B)(v), which would expand the definition of "covered transaction" to include "[t]he contribution (other than through an ordinary customer relationship) by a United States critical technology company of both intellectual property and associated support to a foreign person through any type of arrangement, such as a joint venture, subject to regulations prescribed under subparagraph (C)." While it may be appropriate for the government to review outbound investment transactions involving certain technologies, we believe that the language of Section 3(a)(5)(B)(v) is ill-suited to address the very legitimate national security risks that the bill's proponents have identified.

Specifically, this provision's sweeping scope over companies and transactions that are not likely to present national security issues would prevent CFIUS from focusing its finite resources on the activities most likely to give rise to genuine national security risks. Most if not all of ITI's 63 member companies would be considered "United States critical technology compan[ies]" within the meaning of FIRRMA, regardless of whether they are actually providing, or have the ability to provide, "critical technology" in a given transaction. Moreover, virtually all of these companies "contribut[e] . . . both intellectual property and associated support to a foreign

person" in the normal course of business, often countless times a day. For instance, the cross-border sale of computers, servers, and other hardware coupled with technical support; the licensing of business process software alongside security updates to non-U.S. persons; the provision of cloud computing services internationally; the transfer of trademarks outside of the United States – under the existing language, all of these routine business activities would potentially be subject to CFIUS review. The result would be significant uncertainty among U.S. companies regarding their obligations to file with CFIUS. In the face of such uncertainty, companies would likely err on the side of filing and CFIUS would experience an unmanageable increase in its caseload, with the vast majority of new cases presenting no national security risks at all.

We recognize that FIRRMA specifies that several terms – including "intellectual property," "associated support," and, for practical purposes, "United States critical technology company" – would be defined in regulations promulgated by CFIUS. We also recognize that Section 3(a)(5)(C)(iii) would allow CFIUS to identify in regulations "circumstances in which contributions otherwise described in subparagraph (B)(v) are excluded from the term 'covered transaction' on the basis of a determination that other provisions of law are adequate to identify and address any potential national security risks posed by such contributions." Putting aside the fact that U.S. trade laws already provide multiple tools to address the theft, appropriation, or other improper

use of U.S. intellectual property,[4] we have deep misgivings with this approach. We have no doubt that CFIUS agencies would approach the task of promulgating such regulations with care and rigor, but we believe Congress should define these fundamental concepts rather than defer to the Executive Branch. In our view, the purpose of regulations is to provide additional contour, clarity, and guidance within the four corners of the law set forth by Congress. They should not be a vehicle for the agencies to make policy judgments best reserved to Congress, yet that is essentially what including these undefined terms in the bill would compel the Executive Branch to do.

Perhaps more important, the language of Section 3(a)(5)(B)(v) does not reflect the fact that the national security risks at issue relate to technology and information, not business models and business arrangements. The scenarios that FIRRMA supporters have legitimately raised involve the development in the United States, and the subsequent disclosure to non-U.S. interests, of "foundational," "early stage," "untested," "unfinished," "antecedent," or other kinds of "emerging" technologies. The bill's proponents are reasonably concerned that, without proper oversight, countries hostile to the United States could purchase, access, or otherwise obtain the benefit of those technologies in a manner that could harm U.S. national security.

These are valid concerns, but they have little to do with the particular business context in which they arise. In other words, it does not matter whether an unfriendly power obtains

[4] For example, Section 337 of the Trade Act of 1930, Section 301 of the Trade Act of 1974, and U.S. law implementing the World Trade Organization's Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) all provide tools to address improper use of U.S. intellectual property.

sensitive U.S. technology through an acquisition, joint venture, contract, license, gift, "ordinary customer relationship" (a term not defined in the bill), or other business arrangement. Regardless of the specific business situation, if the potential disclosure of certain technologies raises national security concerns, then we should ensure that our government has the legal tools to resolve those concerns.

Third and finally, we already have the legal tools to address most, if not all, of the national security risks associated with "emerging critical technologies," but we need to ensure that we reinforce those tools with the requisite commitment, creativity, and resources.

A central topic of the debate over FIRRMA involves the relationship between CFIUS and the U.S. export control laws and regulations and, in particular, the extent to which the U.S. export control regime is equipped to address the specific concerns that the bill's proponents have identified. On the basis of extensive discussions with export control experts from our member companies and elsewhere, it is ITI's view that U.S. export control laws and regulations already have the authority to address virtually all, if not all, of the national security risks associated with the contribution or release of "emerging critical technologies" to foreign persons of concern.

We frequently hear the perspective that U.S. export control laws and regulations cannot fully address these risks because they cannot cover the various kinds of "emerging critical technologies" at issue. We take that view seriously but respectfully disagree. The export control laws already apply to any "export" (including releases to foreign persons in the United States and abroad) of technology, knowledge, or other information, at whatever stage of its development, whether it emanates from a company, a physical product, a human being, a piece of software, or

any other medium. Of course, the government needs to identify, describe, and ultimately list as controlled for export that technology, knowledge, or other information of concern, but the legal authorities to do so already exist. Thus, the obstacles to identifying and controlling such emerging technologies of concern are not legal obstacles.

At the same time, we recognize that it is insufficient simply to say that "the export control laws will take care of the problem." It is not enough for our export control regime to be able to address these new national security risks as a matter of law if it cannot do so in practice. Instead, our shared objective ought to be to bolster our existing export control authorities – politically, institutionally, and financially – to ensure that they are well-equipped to meet the challenges of "emerging critical technologies." And we must do so mindful of the frequent and intimate connections between the disclosure of technologies and cross-border business arrangements. In our view, we must build a bridge between the CFIUS world and the export control world in a way that allows each to focus on what it does best, while working together to address novel and complex national security risks.

In months of working with colleagues in Congress, the Executive Branch, and the business community, we and others have spoken of the importance of creating "connective tissue" between FIRRMA and the export control regime. Under this concept, the export control authorities would do the "heavy lifting" to identify, describe, and list "emerging critical technologies," and regulate their release to the destinations, end users, and end uses of concern, while ensuring that CFIUS has meaningful visibility into that process and (if appropriate) the

opportunity to weigh in as well. There are multiple possible ways to build this "connective tissue."

For example, one option for Congress to consider would be to enable FIRRMA to serve as a vehicle for Congress to instruct the Executive Branch to, in essence, "turbocharge" the export control system to meet the evolving technology challenges of today and tomorrow. In particular, this approach envisions the establishment in FIRRMA of a "Subcommittee on Export Controls" to support CFIUS in addressing situations involving "emerging critical technologies." The Subcommittee would serve as a bridge between CFIUS agencies and export control agencies (which already substantially overlap), helping to ensure that the export control system: (a) works vigorously and proactively to identify and describe, and potentially list, "emerging critical technologies;" (b) uses existing legal authorities to unilaterally list "emerging critical technologies" in urgent situations; and (c) seeks to add such technologies to multilateral export control lists, among other functions. (If controls remain unilateral for too long, history has shown that this creates incentives to develop the technology in allied countries without such controls, which ultimately harms the U.S. industrial base.) The ultimate purpose of the Subcommittee would be to enable Congress to ensure that the export control system operates with the creativity, commitment, and aggressiveness necessary to meet the challenges the nation faces, as well as to give CFIUS visibility into how the export control system does so.

We also recommend reviewing how the Export Control Reform Act of 2018 (H.R. 5040), recently introduced by House Foreign Affairs Committee Chairman Royce and Ranking Member Engel, could help to erect this "connective tissue" between CFIUS and the export control system.

We note, in particular, that Section 109 of that bill would direct the President to establish a robust and regular interagency process, involving all key stakeholders from government, industry, and academia, to: (a) systematically identify and describe "emerging critical technologies;" (b) enable the timely listing of such technologies as controlled for export; (c) ensure that the relevant multilateral export control regimes also consider listing such technologies; and (d) provide mechanisms to determine the appropriateness of continued unilateral controls or the eventual removal of such technologies. In short, incorporating Section 109 in some way into FIRRMA would help enable the export control system to address the risks of "emerging critical technologies," while giving CFIUS a window into its doing so.

* * *

Thank you again for inviting me to participate in this discussion. Let me again reiterate ITI's commitment to the success of FIRRMA and to working constructively with this subcommittee and Congress achieve the bill's objectives. I would be pleased to answer any questions you may have.

1101 K Street, NW Suite 610
Washington, D.C. 20005
(202) 737 - 8888 | www.itic.org