Statement of Christopher Padilla
Vice President, Government and Regulatory Affairs
IBM Corporation

Before the Committee on Banking, Housing and Urban Affairs
United States Senate

CFIUS Reform: Examining the Essential Elements

January 18, 2018

Mr. Chairman, Senator Brown and Members of the Committee, thank you for inviting me to testify on this very important topic.

My name is Christopher Padilla, and I am Vice President for Government and Regulatory Affairs at IBM. During the administration of President George W. Bush, I served as Under Secretary of Commerce for International Trade, Assistant Secretary of Commerce for Export Administration, and in other senior roles in the Department of State and the Office of the United States Trade Representative.

In my government roles, I was a senior sub-Cabinet representative of the Commerce Department to the Committee on Foreign Investment in the United States (CFIUS), and I participated closely in inter-agency work to implement new Committee procedures after passage of the Foreign Investment and National Security Act of 2007 (FINSA).

In my role at IBM, I have been involved in two large transactions that were reviewed by CFIUS, and am responsible for the company's worldwide compliance with export controls. My comments today draw upon all these experiences.

IBM shares Congress' goal of strengthening America's national security and appreciates the attempt to do so through the Foreign Investment Risk Review Modernization Act of 2017 (FIRRMA). CFIUS plays an important role in screening inbound foreign investments for potential national security risks, and it is necessary to periodically consider how this process can be improved.

In recent years, IBM has been through three reviews by CFIUS resulting in the successful conclusion of each transaction. From this experience, and from working on mitigation agreements when I served in government, I can assure you that CFIUS has – and makes good use of – its authority to address potential security concerns about inbound foreign investment.

Nevertheless, these experiences also revealed the need for improvements to the CFIUS process, including an expansion of the Committee's jurisdiction to review certain types of inbound

foreign investment transactions. FIRRMA contains some important reforms that IBM supports, such as:

- Expanding the ability of CFIUS to review a limited number of non-passive, but non-controlling, investments;
- CFIUS review of transactions when there are material changes in shareholder rights that expand control or access to information;
- Expanding the ability of CFIUS to review certain real estate transactions when they are in close proximity to military or government installations;
- Taking steps to prevent the deliberate evasion of CFIUS review through complicated financial structures;
- Expanding consultation with allies to coordinate and share information on the types of inbound investment to be scrutinized;
- Ensuring there is a single Senate-confirmed appointee in each CFIUS agency with responsibility and accountability for investment reviews; and
- Providing badly needed resources to the Committee. The CFIUS case load has increased significantly in recent years, and staff resources are already stretched thin. Even if Congress does not elect to give CFIUS an expanded mandate along the lines noted above, it should provide additional resources for CFIUS to do its job effectively.

But the problem with FIRRMA, Mr. Chairman, and a principal reason the bill is controversial in the business community, is that it does something else: it would drastically expand the Committee's mandate beyond examining inbound investment. For the first time, CFIUS would review outbound international commercial activity, including many thousands of non-sensitive IP and technology licensing transactions, even with friendly nations.

This is a serious flaw in the bill that would duplicate and seriously undermine the existing U.S. export control regime, result in a flood of cases that would quickly overwhelm the Committee, and could constitute the most economically harmful imposition of unilateral trade restrictions by the United States in many decades.

Effectively Protecting National Security

As a company with long experience in foreign markets, IBM knows that controlling sensitive technology works best when accomplished internationally, in cooperation with America's allies.

Since the late 1940s, the United States has worked with other countries to stop sensitive technologies from falling into the wrong hands. Whether for dual-use goods like computers and electronics, or for chemicals, aeronautical products, missile technology or nuclear materials, Congress and the executive branch have recognized that to be effective, controls on technology should be multilateral.

A multilateral approach is important for a simple reason: the United States does not have a monopoly on smart people, advanced technologies or investment in leading-edge R&D. Many emerging, dual-use critical technologies are available from other countries, and companies and governments around the world continue to drive the frontiers of technology through their own R&D investments. In fact, in 2017, three-fourths of total global investment in R&D was conducted ***outside*** of the United States[1].

A system of technology controls that unilaterally stops American firms from doing business abroad will not advance national security interests if it simply hands markets to foreign competitors – many of whom are equally capable in advanced technologies.

Yet this is precisely what FIRRMA would do. As drafted, the bill would impose a very onerous – and entirely unilateral – set of restrictions on outbound transactions of U.S. companies involving the "contribution" of technology, intellectual property, and associated support "through any type of arrangement."

This is an exceptionally broad universe that would capture countless licensing, joint development, sales, research, and other transactions involving foreign persons, most of which involve technology that the U.S. government previously determined did not warrant export control restrictions. For example:

- **Computer Hardware Sales & Service:** U.S. firms sell computers, servers and systems worldwide, often paired with installation, maintenance and technical support services. This hardware and related support typically involves hundreds of patented or licensed technologies that would count as a "contribution" of intellectual property under FIRRMA. For example, the sale of a computer server with tech support to a bank in Singapore could come under CFIUS review.

- **Software Licensing:** American technology companies license many types of software applications to both businesses and consumers. These applications often come with technical support that may include help desk, software updates, bug fixes and customization, all of which could involve patented or licensed technologies. For example, the licensing of a database application to a pharmaceutical company in Switzerland could be captured by FIRRMA.

- **Trademarks:** U.S. companies routinely license this most basic form of intellectual property to partners around the world for marketing and business development purposes. This bill could potentially trigger a staggering volume of regulatory filings for basic trademark deals that could not be less threatening to national security.

[1] *2017 Global R&D Funding Forecast*, *R&D Magazine*, Winter 2017 (available at: http://digital.rdmag.com/researchanddevelopment/2017_global_r_d_funding_forecast?pg=1#pg1

Saying that "ordinary customer relationships" are excluded would not solve this overreach, as that term, too, is undefined in FIRRMA and left entirely to the discretion of regulators. Neither is it comforting to be told that regulators will narrow the scope of covered outbound reviews after legislation is passed. Congress, not unelected officials, should decide how broad the CFIUS regulatory remit should be.

More practically, by covering such an extraordinarily broad range of transactions, CFIUS would quickly be overwhelmed with new reviews, making it difficult for the Committee to focus adequately on real threats to national security. Under FIRRMA, the CFIUS workload would skyrocket from about 250 cases per year – already a record number – to many thousands or even tens of thousands, including review of many routine outbound investments and technology transactions hitherto seen as non-threatening by the United States and its allies.

Duplicative Regulation Would Harm U.S. Economic Competitiveness

As drafted, FIRRMA would turn CFIUS into a supra-export control agency, duplicating long-standing U.S. export control regimes and unilaterally limiting the ability of American firms to do business around the world. Foreign competitors that do not face similar regulatory restrictions will seize global market opportunities while American companies are left watching from the sidelines.

FIRRMA would give CFIUS extremely broad discretion to define the scope and reach of its regulatory authority, creating uncertainty and delays in investment decisions, contract negotiations and sales to foreign customers.

This approach stands in stark contrast to the approach recently taken by Congress and the Administration to curtail duplicative bureaucracy and regulation, and could capture under government control a very wide range of commercial activity. As a result, foreign customers and investors will look elsewhere, and over the long term this could drive innovation and the development of new critical technologies outside the United States.

Protecting National Security Using Existing Authorities

One of the issues driving FIRRMA is a concern that the current CFIUS and export control regimes do not address the issue of emerging critical technologies. There is some justification for this concern. However, there is existing regulatory authority to impose new technology controls quickly, while also ensuring that effective, long-term controls are established in partnership with U.S. allies.

In 2012, a final rule was published (15 CFR 742.6(a)(7)) which established the "0Y521" series of controls in the Export Administration Regulations (EAR). Under this little-used regulation, the government can impose immediate controls on emerging or other technologies if deemed in the national security or foreign policy interests of the United States. Crucially, however, this regulation also envisions that the United States will simultaneously pursue effective multilateral

controls for these technologies with U.S. allies. And such controls would be administered through the specific, parameter-based, and relatively transparent process of export licensing that the business community knows and can work with.

So, mechanisms exist to quickly control sensitive technologies if necessary. But which technologies should be so controlled? This is where the picture gets murkier.

Technology control lists are badly in need of a refresh, and Congress should consider using its oversight authority to make this happen. Under the Export Administration Act, Congress directed that regular list review should be a priority, and it established the Militarily Critical Technologies List (MCTL) in statute for just that purpose. Yet a GAO report in February 2015 found that "the MCTL was out-of-date and was no longer being published online, but that widespread requirements to know what is militarily critical remained.[2]" The same report found:

> "*According to DOD officials responsible for the MCTL, they are no longer updating the list, and are in the process of determining whether it is appropriate to seek relief from the requirement to maintain the list. They stated that alternatives to the MCTL are being employed based on the specific needs of each agency, and DOD offices are using the U.S. Munitions List, the Commerce Control List 600 Series, and the Industrial Base Technology List as alternatives to the MCTL.*"[3]

This is not how Congress thought the process should work. Using the control list to say what is militarily critical puts the cart before the horse. The intent was that the Defense Department, working with other agencies and with industry, would broadly identify general categories of militarily critical technologies (including emerging technologies of concern) in the MCTL, and then draw from that list to propose specific, parameter-based, and usually multilateral export controls. The controls would be implemented via the Commerce Control List, the U.S. Munitions List, and international control regimes such as COCOM (succeeded by the Wassenaar Arrangement), the Missile Technology Control Regime, the Australia Group, the Nuclear Suppliers Group, or others. Export controls have worked well to protect national security for decades, but the list review process has recently fallen into disuse.

FIRRMA would not correct this problem, and in fact could make it worse. Under FIRRMA the government would define some new, very vague and broad list of technologies of concern (even though it has failed to update technology lists already required under current law) and then wait until something pops up in a transaction review. The government might then try to stop it – but only unilaterally, on a deal-by-deal basis, and without regard to foreign availability, technology trends, or consultation with allies or industry. Casting an extraordinarily wide net over routine commercial transactions and applying, in effect, a regulatory test of "we'll know it

---

[2] U.S. Government Accountability Office, "*Critical Technologies: Agency Initiatives Address Some Weaknesses, But Additional Interagency Collaboration is Needed*", February 2015, GAO 15-288.

[3] Ibid., and reference is also made to a prior report: U.S. Government Accountability Office, "*Protecting Defense Technologies: DOD Assessment Needed to Determine Requirement for Critical Technologies List*", January 2013, GAO-13-157.

when we see it" would be deeply damaging to U.S. competitiveness, and, more important, could lead to a false sense of security.

Instead, there should be a return to a more disciplined list review and multilateral export control process already mandated by law. Congress could act to ensure effective monitoring and control of emerging technologies through existing export regulations by requiring:

1) regular, ongoing reviews of emerging technologies for potential national security risks as envisioned by the MCTL;
2) full and robust application of existing EAR regulatory authorities to control these emerging technologies as necessary to protect national security; and
3) annual reports to Congress with additional oversight to ensure that this export control process effectively addresses any risks.

Conclusion

In summary, IBM fully supports efforts to strengthen national security. We encourage Congress to find ways to do so without undermining U.S. economic competitiveness, or driving innovation and investment outside the United States.

We believe that a refreshed technology control list, and the more robust use of existing export control authority ultimately leading to international controls, would be the most effective way to protect national security interests.

While FIRRMA contains several important reforms to CFIUS, the Committee should continue to focus on inbound foreign investment in the United States, rather than reviewing outbound transactions that are low-risk or already covered under existing export control regulations.

Thank you for this opportunity to appear before the Committee. I would be pleased to answer any questions that you might have.