AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

WASSENAAR: CYBERSECURITY AND EXPORT CONTROLS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

AND THE

SUBCOMMITTEE ON CYBERSECURITY,
INFRASTRUCTURE PROTECTION,
AND SECURITY TECHNOLOGIES

OF THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

SECOND SESSION

JANUARY 12, 2016

Serial No. 114–102
(Committee on Oversight and Goverment Reform)

Serial No. 114–49
(Committee on Homeland Security)

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

23–401 PDF WASHINGTON : 2017

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Iowa
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DeSAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

JENNIFER HEMINGWAY, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
TROY STOCK, *IT Subcommittee Staff director*
SHARON CASEY, *Deputy Chief Clerk*

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona

ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

COMMITTEE ON HOMELAND SECURITY

MICHAEL T. MCCAUL, Texas, *Chairman*

LAMAR SMITH, Texas
PETER T. KING, New York
MIKE ROGERS, Alabama
CANDICE S. MILLER, Michigan, *Vice Chair*
JEFF DUNCAN, South Carolina
TOM MARINO, Pennsylvania
LOU BARLETTA, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
JOHN KATKO, New York
WILL HURD, Texas
EARL L. "BUDDY" CARTER, Georgia
MARK WALKER, North Carolina
BARRY LOUDERMILK, Georgia
MARTHA MCSALLY, Arizona
JOHN RATCLIFFE, Texas
DANIEL M. DONOVAN, JR., New York
BENNIE G. THOMPSON, Mississippi
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BRIAN HIGGINS, New York
CEDRIC L. RICHMOND, Louisiana
WILLIAM R. KEATING, Massachusetts
DONALD M. PAYNE, JR., New Jersey
FILEMON VELA, Texas
BONNIE WATSON COLEMAN, New Jersey
KATHLEEN M. RICE, New York
NORMA J. TORRES, California

BRENDAN P. SHIELDS, *Staff Director*
JOAN V. O'HARA, *General Counsel*
MICHAEL S. TWINCHEK, *Chief Clerk*
I. LANIER AVANT, *Minority Staff Director*
MADELINE EDA MATTHEWS, *Professional Staff member*

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

JOHN RATCLIFFE, Texas, *Chairman*

PETER T. KING, New York
TOM MARINO, Pennsylvania
SCOTT PERRY, Pennsylvania
CURT CLAWSON, Florida
DANIEL M. DONOVAN, JR., New York
MICHAEL T. MCCAUL, Texas *(ex officio)*
CEDRIC L. RICHMOND, Louisiana
LORETTA SANCHEZ, California
SHEILA JACKSON LEE, Texas
JAMES R. LANGEVIN, Rhode Island
BENNIE G. THOMPSON, Mississippi *(ex officio)*

BRETT DEWITT, *Subcommittee Staff Director*
JOHN DICKHAUS, *Subcommittee Clerk*
CHRISTOPHER SCHEPIS, *Minority Subcommittee Staff Director*

CONTENTS

Page

Hearing held on January 12, 2016 1

WITNESSES

Mr. Vann H. Van Diepen, Principal Deputy Assistant Secretary for International Security and Nonproliferation, Department of State
Oral Statement 10
Written Statement 12
Hon. Kevin J. Wolf, Assistant Secretary for Export Administration, U.S. Department of Commerce
Oral Statement 17
Written Statement 19
Ms. Phyllis Schneck, Deputy Under Secretary for Cybersecurity and Communications, National Protection and Programs Directorate, U.S. Department of Homeland Security
Oral Statement 23
Written Statement 25
Ms. Cheri Flynn McGuire, Vice President, Global Government Affairs and Cybersecurity Policy, Symantec
Oral Statement 30
Written Statement 32
Mr. Iain Mulholland, Vice President, Engineering Trust and Assurance VMWARE, Inc.
Oral Statement 44
Written Statement 46
Ms. Cristin Flynn Goodwin, Assistant General Counsel, Cybersecurity, Microsoft Corporation
Oral Statement 51
Written Statement 53
Mr. Dean C. Garfield, President and CEO, Information Technology Industry Council
Oral Statement 64
Written Statement 66
Ms. Ann K. Ganzer, Director of Conventional Arms, Threat Reduction, Bureau of International Security and Nonproliferation, Department of State
Oral Statement 74

APPENDIX

Representative Sheila Jackson Lee Opening Statement 96
2015–12–16 Members of Congress to Ambassador Rice re Wassenaar 102
2015–07–20 Members of Congress to Wheeler-DOC re Wassenaar 113
2016–01–12 Mr. Beckerman-Internet Association re Wassenaar 116

WASSENAAR: CYBERSECURITY AND EXPORT CONTROLS

Tuesday, January 12, 2016

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM, JOINT
WITH SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE
PROTECTION, AND SECURITY TECHNOLOGIES, COMMITTEE ON
HOMELAND SECURITY,
Washington, D.C.

The subcommittees met, pursuant to call, at 2:23 p.m., in Room 2154, Rayburn House Office Building, Hon. Will Hurd [chairman of the Subcommittee on Information Technology] presiding.

Present for Subcommittee on Information Technology: Representatives Hurd, Farenthold, Walker, Blum, Kelly, Connolly, and Lieu.

Present for Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: Representatives Ratcliffe, Marino, Perry, Clawson, Donovan, McCaul (ex officio), Richmond, Sanchez, Jackson Lee, Langevin, and Thompson (ex officio).

Mr. HURD. The Subcommittee on Information Technology of the Committee on Oversight and Government Reform and the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies of the Committee on Homeland Security will come to order. Without objection, the chair is authorized to declare a recess at any time. I would like to start off by recognizing my friend and the chairman of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, and fellow Texan, the Honorable Ratcliffe, John Ratcliffe. Over to you, sir.

Mr. RATCLIFFE. I thank the gentleman for yielding. The purpose of this hearing is to address the impact of the Wassenaar Arrangement, which was recently amended to propose export controls for cybersecurity products. I now recognize myself for an opening statement.

The House Homeland Security Committee's Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies and the House Oversight and Government Reform's Subcommittee on Information Technology meet today to hear from key industry and government stakeholders about the impact of the Wassenaar Arrangement, that it will have on American people, on American businesses, and on the cybersecurity industry.

I first want to start off by thanking my friend, Mr. Will Hurd, the gentleman from Texas, for co-chairing this hearing. Today, we are doing what Americans would like to see more of in Congress. Two committees that don't often work together are able to, and

happy to come together to tackle an issue that's extremely important and relevant to national security and to the security of individuals' personal information. Congressman Hurd and I share the belief that one of our core duties here in Congress is to bypass the jurisdictional roadblocks, and make real progress towards keeping our citizens safe.

To the issue at hand, we know that private industry in America is excellent at responding to consumer demands. Many companies, including some of those here today, pride themselves on guaranteeing the security of their customers' personal information. Others represented here exist solely to help in securing that information. They also secure vital sectors of society such as critical infrastructure and the financial sector. Their success hinges, in part, on their ability to guarantee their own security. Today, I hope to hear from our witnesses on how the Wassenaar Arrangement in its implementation would affect these objectives.

The Wassenaar Arrangement was established 20 years ago to apply to conventional arms and dual-use goods and technology. Changes made in 2013 sought to extend export controls to cybersecurity intrusion and surveillance software and technology.

These changes were motivated by a desire to prevent authoritative regimes from repressing their people. This intent is noble. If the administration's implementation effort resulted in unified dissent from the technology and cybersecurity industries, from academics and researchers, the energy and financial sectors also voiced deep concerns. And they were echoed by civil society groups who said that the proposal could make communicating about security vulnerabilities almost impossible in certain cases. The Federal Government engages in countless ways with the American people and our international partners. When proposing actions, the government should, at a minimum, not do harm to its own people. I'm interested to hear from our government witnesses how they believe this arrangement will successfully deter the accumulation of digital weapons, which aren't constructed in factories, which don't need physical space for storage, and which don't depend on traceable means of transport.

I hope to better understand how they believe this export control framework can be effectively applied to intrusion software. I agree that we should strive to limit dangerous technologies from falling into the hands of bad actors. But national security and Americans' personal security can't be sacrificed in the process. There are many ways the United States strives to combat human rights violators. And I hope to hear today why this route wasn't chosen over other options. As we can see by the variety and the size of our witness panel, the Wassenaar Arrangement has broad implications. Recent reports and the witness testimony today demonstrate that we are far from a consensus on this issue. The administration's top three stated priorities include, and I quote, "protecting the country's critical infrastructure from cyber threats, improving our ability to identify and report cyber incidents, and engaging with international partners to promote Internet freedom, and building support for an open, interoperable, secure, and reliable cyberspace."

I assume that our government witnesses are well-versed in these goals and their prioritization. Yet, in reading the comments to the

proposed rule and general thoughts on the cybersecurity section of the Wassenaar Arrangement, one sees a probable contradiction in the first two goals. Additionally, I think it's unlikely that this arrangement achieves the open and interoperable cyberspace that is in the public's interest. If we are to expect the cybersecurity provisions of this arrangement to be workable, we need to make sure that our stated intentions and actions are not contradictory. If we can't do that, I question why as a country we are agreeing to this updated arrangement.

Just last month, Congress passed legislation to encourage the sharing of cyber threat information. Both the private sector and the Government stand to benefit from the increased flow of valuable cyber-threat information. Today, we need to hear whether the Wassenaar Arrangement would have a counterproductive impact on such sharing, and whether it would undermine the law that the President just signed. As a Nation, we advocate for human rights, and we assist those harmed by authoritarian regimes. However, we must, first and foremost, safeguard the security of our Nation and our citizens.

I look forward to hearing from the witnesses about the best path forward and how we can come together to best protect the American people. And I yield back.

Mr. HURD. It's now my pleasure to recognize the distinguished gentleman from the great State of Louisiana, Mr. Richmond, the ranking member of the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, for his opening statement. Mr. Richmond, you're recognized for 5 minutes.

Mr. RICHMOND. Thank you, Chairman Hurd and Chairman Ratcliffe, also Ranking Member Kelly, for convening this joint hearing on U.S. rulemaking regarding cybersecurity technology issues in the Wassenaar Arrangement. I also want to thank our panel of witnesses today, both the government and industry representatives.

The Wassenaar Arrangement consists of America's efforts, in collaboration with 40 of our trading partners, to put into place export controls for conventional arms and dual-use goods and technologies. As we know, dual-use goods and commodities, processes are technologies used primarily for civilian purposes, which can also be used to develop or enhance the capabilities of military equipment or initiatives. We find ourselves in rapidly changing times. And dual-use goods and technologies now encompass cybersecurity technologies, which are vital in protecting private, commercial, and governmental data, and protecting the operation of our information networks, both public and private. The 41 nations participating in the Wassenaar Arrangement agreed to include cybersecurity issues. And the United States has led the way.

The Department of Homeland Security's Cybersecurity and Communications Office, within the National Protection and Programs Directorate, is the storehouse of a great deal of our Nation's civilian cybersecurity expertise. And I'm glad to see Dr. Schneck as one of our witnesses today, and look forward, especially, to her perspective.

I found it helpful to frame the cybersecurity issues contained in the Wassenaar Arrangement as a series of questions. Does the pro-

posed rule fulfill its intended goal? Does the proposed rule have any negative unintended side effects? Will modification of the proposed rule address concerns adequately?

And, finally, should the Wassenaar provision be renegotiated, or an alternative be found? If the critics of the wording of the current proposed rulemaking are right, then I'm sure the answers will be no, yes, no, yes. According to a large number of professionals, the expert restrictions for the defined cybersecurity products and technologies in the rule may certainly reduce the likelihood of repressive governments obtaining surveillance technology through legal sources, but the criminal underground would not be subject to such restrictions. And such repressive regimes might switch to those suppliers.

But let us not speculate. While my subcommittee does not appear to have any immediate legislative or oversight jurisdiction on this matter, testimony today from industry and government agencies involved, would help us to learn about the impacts of the proposed rule as drafted and how it will affect or impede not only research on the specifics of cybersecurity, but possible effects on the larger global cybersecurity community.

Mr. Chairman, at this time, I would like to yield 1–1/2 minutes to Mr. Langevin, who has been a leader and an expert in our caucus on this issue.

Mr. RATCLIFFE. [presiding.] The gentleman is recognized.

Mr. LANGEVIN. Thank you, Mr. Chairman. I want to thank the ranking member, Ranking Member Richmond, for yielding the time. And I want to thank both chairmen and ranking members of the committee for holding this hearing. I've been closely following the intrusion software additions since BIS proposed the original rule last May. In July, several of my colleagues joined me in voicing our concerns with that regulation as part of the public comment period. And last month, 125 members joined Chairman McCaul and me in a bipartisan effort in highlighting some of those thoughts in a letter to the President's National Security Advisor.

Throughout this period, I've been thoroughly impressed by Bureau of Industry and Security's efforts to be as open as possible during the rulemaking process. And I commend you, Assistant Secretary Wolf, and your staff, for your willingness to listen to constructive feedback. I thank you for your work in that respect. I think all of us here today believe that intrusion software can be dangerous in the wrong hands. But the original proposed rule had many unintended consequences that must be addressed. I hope we will explore those barriers during this hearing, which could be detrimental to both our economic competitiveness and our national security, and that we will also come out with a clear understanding of the way forward and how to better incorporate stakeholder feedback from the outset in future rulemaking.

With that, I would like to, again, thank Chairmen Ratcliffe and Hurd and Ranking Members Richmond and Kelly for addressing this very important topic. And I'll submit my full statement for the record. And I would yield back the balance of my time.

Mr. RICHMOND. And with that, Mr. Chairman, I will yield back the balance of my time.

Mr. RATCLIFFE. I thank the gentlemen from both Louisiana and Rhode Island. The chair now recognizes the chairman of the Homeland Security Committee, my friend, the gentleman from Texas, Mr. McCaul.

Mr. MCCAUL. I thank the gentlemen from Texas, both Mr. Ratcliffe and Mr. Hurd, for having this hearing today on a very important issue. It's consequential. Strengthening our Nation's cybersecurity is of the upmost importance right now, and will determine our Nation's position as a world leader in the future. The playing field for international conflict is constantly evolving. Cyber attacks can come from anywhere at any time, and without any prior notifications.

As chairman of the Homeland Security Committee, keeping Americans safe is my primary concern. And that is no simple task in such a dynamic environment. Unfortunately, the amendment to the Wassenaar Arrangement would depreciate the research, development, and deployment of important tools that we all use every day to secure against cyber attacks.

The United States has a duty to be a world leader. The establishment of a multi-national arrangement to restrict the trade of conventional arms and dual-use goods and technologies has only been possible through strong American leadership. To continue fulfilling this imperative role, the United States must ensure that such agreements support technically and practically intelligent policies on cybersecurity.

If the matter at hand was simply a question of efficacy, we wouldn't be here today. If the only concern was that the Wassenaar Arrangement might have room for improvement, this conversation would be very different. But what has been violated here is the fundamental adage of do no harm. The State Department agreed to an arrangement that would restrict a group of information security tools and products. This agreement and the proposed implementation could hobble the entire cybersecurity ecosystem, as well as cross-border data flows, and global collaboration that support it. Weakening our cyber researchers and innovative service providers is bad enough. But as we have seen again and again, any weakness in our cyber posture will percolate to other industries and harm individual Americans.

Furthermore, under the arrangement, participating States already exchange specific information on a regular basis about global transfers of certain goods and technologies. Part of the Wassenaar Arrangement is looking at that information to find dubious acquisition trends. I don't see any limitation on the ability of the Wassenaar Arrangement to pursue the stated goals of increased transparency without adding burdensome and counterproductive licensing requirements.

I hope that the witnesses are able to speak today about why the addition of intrusion software language to the arrangement was preferred as the best means of achieving American goals, instead of other options, such as through sanctions, which would address bad actors more directly without unintended consequences.

Lastly, the Homeland Security Committee worked hard in putting together and shaping information, sharing legislation which was signed into law in December. That legislation facilitates a

sharing of cyber information between the Federal Government and the private sector to assist security experts and others in rapidly identifying and resolving vulnerabilities that threaten the security of our networks.

We must not backtrack on this progress. It is a priority of the Homeland Security Committee to investigate whether the domestic execution of the relevant cybersecurity section of the Wassenaar Arrangement would obstruct positive collaboration on cybersecurity that protects American information and information systems.

I hope the backlash received and the response here in the Congress will prevent the State Department from attempting to take momentous negotiations upon themselves without consultation from the stakeholders in the future. The administration must not ignore the serious, broad implication of the results. What we won't stand for is a de facto regulation of a thriving sector and cornerstone of American industry, an industry that provides the tools that we all, including governments, use to secure ourselves. I expect this hearing today will send an important message that the intrusion software language in the Wassenaar Arrangement is simply unworkable. We, in the Congress, expect that the administration will work to correct the serious issues in this arrangement moving forward. Again, I want to thank the chair and ranking member for holding this hearing. And I yield back.

Mr. RATCLIFFE. Thank the chairman. The chair now recognizes the ranking member of the Oversight and Government Reform Subcommittee on Information Technology, the gentlelady from Illinois, Ms. Kelly.

Ms. KELLY. Thank you, Mr. Chairman. Welcome to the witnesses participating in today's hearing on export controls for certain cybersecurity tools. The export controls for intrusion and surveillance technologies agreed to at the Wassenaar Arrangement were intended to help prevent repressive regimes from obtaining and using intrusive technology against their own citizens. These are important human rights objectives. It is also critically important that U.S. cybersecurity policies advance our overall efforts to protect information and systems from cyber attacks and data breaches.

Today's hearing is recognition of the fact that the Federal Government and private sector must work together effectively to thwart cybercrime. The Bureau of Industry and Security's proposed rule to implement the Wassenaar Arrangement's export controls on cybersecurity intrusion, and surveillance items could seriously hinder the cybersecurity industry and our national security. The language in the proposed rule would interfere with the ability of businesses and of the Federal Government to acquire and utilize cybersecurity tools that are critical to the security of information systems and data, and frustrate the real-time information sharing of vulnerability, which is relied upon to prevent or to stop a cyber attack.

Going forward, BIS and its interagency partners should reconsider their policy approach to this rulemaking, so that the export controls do not negatively affect our Nation's ability to defend against cyber threat and the policy conforms with the broader U.S. cybersecurity strategy and national security.

The Information Technology Subcommittee has held multiple hearings examining the nature of cyber threats and how to enhance the security of information and information networks. We have learned that no company or industry is immune from cyber attacks, and that cyber attackers are highly sophisticated, and constantly evolving their tactics.

We are all aware of the major breaches that American companies, contractors, and government agencies have sustained in recent years. Given this persistent threat to information systems, it is critically important that the U.S. policies and regulations are designed to enhance the tools and capabilities that ensure the security of critical information targeted by cyber attackers.

Last month, the Democratic members of this subcommittee, along with 120 other Members of Congress, signed onto a bipartisan letter to National Security Advisor Susan Rice, requesting the WhiteHouse's collaboration and advice in the development of export control policies for cybersecurity tools. In that letter, we expressed our concerns that the proposed rulemaking pertaining to export controls of intrusion software and vulnerability research could reduce the ability of private businesses and the Federal Government to defend against cyber threats and impair national security efforts.

I would like to commend BIS for anticipating the need to assess the impact of the export controls on the cybersecurity industry and requesting public comment on the effects of this proposed rule. The Bureau is currently reviewing the 264 public comments it received.

I look forward to hearing from today's witnesses on the impact of this proposed rule and discussing a path forward that achieves the human rights objectives of the export controls without negatively affecting innovation and research on cybersecurity tools and vulnerability. Thank you, Mr. Chairman. And I look forward to the witnesses' testimony.

Mr. RATCLIFFE. I thank the gentlelady. The chair now recognizes the ranking member of the Homeland Security Committee, the gentleman from Mississippi, Mr. Thompson.

Mr. THOMPSON. Thank you very much. Thank you, Chairman Hurd, Ranking Member Kelly, Chairman Ratcliffe, and Ranking Member Richmond, for your leadership in calling this joint subcommittee hearing today. I particularly want to thank the distinguished panel of witnesses before us today. You all play an important role in America's vital trade and business life. And I'm grateful you took the time to come help us understand a very complicated issue.

The concept of cyber and information security is fundamental to our economy across all sectors, not only for business computers and networks, but also because the issue crosses the lanes of private, personal information, and policies that governance consideration. Cyber and information security are also issues that involve the ingenuity and initiative that makes American entrepreneurs and computer software scientists leaders in the world market.

The Wassenaar Arrangement for the export control of dual-use cybersecurity products is not only technically complex, but also involves moral and ethical considerations that must be taken into account.

The United States economy is the largest in the world and the most creative, innovative, and productive. The strength of our engineers, scientists, and industrial leaders and across all sectors of American industry is unmatched. While the American worker is recognized as the most productive worker in the world, the electronic world dominates our business, information, security processes. And we depend most heavily on effective functioning of machine and computer system controls to achieve our high level of productivity. We cannot maintain these high levels of productivity without comprehensive and massive security efforts to protect not only machines and computers, but the electronic networks that we all depend on in our daily lives, ones that sustain the highest standard of living in the world for American families.

The United States leads the world in the production of cybersecurity products and systems that not only produce the software applications that keep our economy running, but also the information security products that protect our vital personal data, business information, and communications network. The treaties, agreements, and arrangements we have with our international trading partners play a fundamental role in allowing our U.S.-made products to be exported easily and without interference. And those are often intricate and detailed provisions. I am very pleased we are holding this hearing to learn more about one of the most complex issues facing international trade today. I look forward to the testimony of our witnesses. With that, I yield back.

Mr. RATCLIFFE. I thank the ranking member for his remarks. The chair how recognizes the chairman of the Oversight and Government Reform Subcommittee on Information Technology, my good friend from Texas, Mr. Hurd.

Mr. HURD. Mr. Chairman, thank you. And I look forward to getting this institution focused on solving problems rather than jurisdictional issues. And I would like to thank Chairman McCaul and Chairman Chaffetz for their leadership and Ranking Members Thompson and Cummings for working on issues like this in a bipartisan fashion. It's great working alongside you, Mr. Richmond. And I would especially like to thank my good friend, Robin Kelly, for her partnership over the last year. And I'm looking forward to working together with you this year.

This is an important topic, eight panelists, a bunch of chairmen, a bunch of subcommittee chairmen, a lot of ranking members. And one of the reasons is that it's been estimated that 97 percent of all Fortune 500 companies have been hacked, and the other 3 percent have been and just don't know it. And this is the size and scope of the cyber problems this Nation is facing. BlueCross BlueShield, Anthem, most recently, Juniper Networks and OPM, where the sensitive PII of 21.5 million Americans whose data was stolen are just a few examples of the ongoing digital threat our Nation faces every single day.

Our adversaries are constantly targeting our information technology. And in doing so, they steal our intellectual property, healthcare data, and the most private details of the lives of millions of Americans. So when in May of last year, the Bureau of Industry and Security at the Department of Commerce published a draft rule implementing an export control regime on some of the

most basic cybersecurity tools and methods, I became deeply concerned about the potential for unintended circumstances and consequences.

The truth is that cyber weapons are not analogous to conventional weapons that the Wassenaar Agreement has been discussing and regulating since its inception. The same code that can be used to steal, disrupt, or destroy can also be used to protect. My concern, a concern shared by many of those companies and experts who submitted comments to BIS over the summer, is that the language of the proposed rule is so broad and vague that if implemented, it would do profound damage to our Nation's cybersecurity posture. The IT Subcommittee is very interested in the process that the State Department employed when adding these highly technical and complex cybersecurity items to the Wassenaar's export control regime, were experts, the cybersecurity industry, or the IT community at large, included in the discussions leading up to the agreement? If not, why? And how can we make sure they are consulted in the future so this kind of thing doesn't happen again.

Cybersecurity practitioners have to move at the pace of technology. They cannot stop and wait to push a critical patch out to their international partners or clients who are left vulnerable while regulators delay and bureaucrats impose mountains of red tape. In the cybersecurity business, the clock starts when you know you've got an indicator of compromise and doesn't stop until you know it's been patched. In no time at all, a vulnerability can be exploited and data extracted. With months, hackers can take their time and do unspeakable damage to American interests.

One of the reasons the IT Subcommittee exists is to examine the impacts information technology has on our laws, governmental structures, society writ large, and our regulatory approach.

The question here today is not only whether or not the Wassenaar nations need to re-think and re-draft those cyber tool controls, but also, whether or not an export control regime is the correct institution to solve the problem of keeping dangerous digital tools out of the hands of despots. I thank Chairman Ratcliffe for his shared interest in this issue. And I look forward to today's discussion. And I yield back.

Mr. RATCLIFFE. I thank the gentleman from Texas. Other members are reminded that opening statements may be submitted for the record. And as noted by others, we are pleased today to have with us a very distinguished panel of witnesses on an important topic, including Mr. Vann Van Diepen, the principal Deputy Assistant Secretary for the Bureau of International Security and Nonproliferation at the U.S. Department of State; Ms. Ann Ganzer, the Director of Conventional Arms Threat Reduction for the Bureau of International Security and Nonproliferation at the U.S. Department of State; the Honorable Kevin Wolf, the Assistant Secretary for Export Administration at the U.S. Department of Commerce; Dr. Phyllis Schneck, the Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate at the U.S. Department of Homeland Security; Ms. Cheri Flynn McGuire, the vice president for Global Government Affairs and Cybersecurity Policy at Symantec; Mr. Iain Mulholland, the vice president for Engineering Trust and Assurance at VMware;

Ms. Cristin Flynn Goodwin, the assistant general counsel for Cybersecurity at Microsoft; and, finally, Mr. Dean Garfield, the president and CEO of the Information Technology Industry Council.

Thank you all for being here today. The witnesses' full written statements will appear in the record. And at this time, I would ask all of the witnesses to stand and raise your right hand so that I can swear you in for your testimony.

Do each of you swear or affirm that the testimony you are about to provide today shall be the truth, the whole truth, and nothing but the truth so help you God? Let the record reflect that the witnesses answered in the affirmative. The chair now recognizes Mr. Van Diepen for his opening statement.

WITNESS STATEMENTS

STATEMENT OF VANN H. VAN DIEPEN

Mr. VAN DIEPEN. Thank you, Chairman Hurd and Chairman Ratcliffe, Ranking Members Kelly and Richmond, and members of the committees, for the opportunity to talk today about export control efforts in the challenging new area of cyber tools. As we've heard from you all, we hear almost daily about malicious cyber activities that disrupt businesses, compromise privacy, or threaten national security.

Congress itself has also recognized the overall cybersecurity threat in legislation. The 2014 National Defense Authorization Act required developing an integrated policy to control the proliferation of what it termed "cyber weapons," including through multilateral enforcement activities and diplomatic engagement. To be most effective, export controls should be multilateral. The Wassenaar Arrangement has the responsibility for multilateral national security export controls on dual-use items not related to weapons of mass destruction, such as cyber tools. This 41-country regime was established in 1996 to contribute to regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and related dual-use goods and technologies, thus preventing destabilizing accumulations.

Upholding our international export control commitments is central to our ability to get other countries to uphold theirs, not just in Wassenaar, but in the nuclear, chemical, biological, and missile control regimes as well. Because these same cyber tools can also be used for beneficial purposes, such as identifying vulnerabilities and improving cybersecurity, we need to strike the appropriate balance in implementing such controls to promote national security objectives, while making sure that the controls' benefits clearly exceed any commercial or national security costs.

Recognizing the challenge in implementing the cyber control, the U.S. Government took the uncommon step of going through a public notice and comment process. The comments were instructive. And we take them very seriously. It is clear from the comments received that the first version of the proposed U.S. rule to implement the Wassenaar control missed the mark. And the interagency continues to work through the concerns raised.

Fortunately, the cyber control is included on the least sensitive portion of the Wassenaar list. This provides us with substantial flexibilities we can employ in the process of implementing that control nationally, just as most other Wassenaar members have done in already having implemented the cyber control for over a year without apparent controversy.

We appreciate your committee's interest in this issue. And we are committed to working closely with all the other stakeholders in the interagency, as well as industry, and the other relevant external stakeholders, to seek a balanced way forward that meets our important policy objectives while addressing the concerns raised. Thank you.

[Prepared statement of Mr. Van Diepen follows:]

Statement of
Vann H. Van Diepen
Principal Deputy Assistant Secretary
for International Security and Nonproliferation
U. S. Department of State

Before the

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

And the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

January 12, 2016

Thank you, Chairmen Hurd and Ratcliffe, Ranking Members Kelly and Richmond, and Members of the Committees, for the opportunity to talk to you today about nonproliferation export control efforts in the new area of cyber tools. This is a very challenging area. We hear almost daily about malicious cyber activities that disrupt businesses, compromise privacy, or threaten national security. The 2014 destructive malware attack on Sony Pictures Entertainment and recent high profile intrusions involving the exfiltration of sensitive data from government and private sector computers highlight the kinds of cyber threats we now face. These dangers are only increasing as the tools for carrying out these actions in cyberspace become more widely available and more powerful.

While these cyber tools enable breaches of networks and data for malicious purposes, they can also be used for beneficial purposes, such as identifying vulnerabilities and improving cybersecurity. The private sector and security research community play a critical role in promoting cybersecurity, and it is important that they continue to innovate in this dynamic technological space.

Congress itself has recognized the overall cybersecurity threat that our nation faces, and it has sought to specifically address the dangers posed by the uncontrolled spread of capabilities to carry out malicious activity in cyberspace. In the 2014 National Defense Authorization Act, Congress required the President to develop an integrated policy to control the proliferation of what it termed "cyber weapons" though unilateral and multilateral enforcement activities, financial means, and diplomatic engagement.

To be most effective, export controls should be multilateral; obviously, it is easier to evade just the controls of the United States than those of dozens of countries. The Wassenaar Arrangement has the responsibility for multilateral national security export controls on dual-use items not related to weapons of mass destruction (WMD), such as cyber tools. This 41-country regime was established in 1996 to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms

and related dual-use goods and technologies, thus preventing destabilizing accumulations, including by terrorists.

Over Wassenaar's 20-year history, it has contributed to national and international security by establishing control lists and best practices that have led to its Participating States preventing transfers of arms and sensitive dual-use items to countries and programs of concern. The concerted efforts of its members in controlling the items on its lists, and keeping those lists up to date, is a critical component of U.S. and international security. The Wassenaar control lists, along with those of the WMD and missile nonproliferation regimes, form the backbone of the U.S. dual-use control system.

The United States is a global leader in nonproliferation, including in Wassenaar. We have pressed consistently for controls on a range of dual-use technologies that, when used appropriately, can protect us, but can also be used against us, including things like lasers and sophisticated electronics. When all 41 members, as well as the growing number of non-member countries that adhere unilaterally to Wassenaar controls, work together to control sensitive technologies, we can better keep these items out of the hands of those who would use them against us -- while preserving their use in legitimate trade.

We need to strike the appropriate balance in implementing such controls to promote national security objectives while making sure that the controls' benefits

clearly exceed any commercial or national security costs. Upholding our international export control commitments is central to our ability to get other countries to uphold theirs, not just in Wassenaar but in the WMD and missile control regimes as well.

Recognizing the challenge in implementing the cyber control, the U.S. government took the uncommon step of going through a public notice and comment process. Usually, Wassenaar controls get implemented through a final rule. The U.S. government made this decision because we wanted to give industry and the research community an opportunity to provide their views and wanted to make sure we get U.S. implementation right. The comments were instructive, and we take them very seriously. It is clear from the comments received that the first version of the proposed U.S. rule to implement the Wassenaar control missed the mark, and the interagency continues to work through the concerns raised.

Fortunately, the cyber control is included on the least sensitive portion of the Wassenaar list. This provides us with substantial flexibilities we can employ in the process of implementing that control nationally, just as most other Wassenaar members have done in already having implemented the cyber control for over a year without apparent controversy.

We appreciate your Committees' interests in this issue, and we are committed to working closely with Commerce and all other stakeholders in the

interagency, as well as industry and the other relevant external stakeholders, to seek a balanced way forward that meets our important policy objectives while addressing the concerns raised.

Mr. RATCLIFFE. Thank you, Mr. Van Diepen. The chair now recognizes the Honorable Kevin Wolf for his statement.

STATEMENT OF HON. KEVIN J. WOLF

Mr. WOLF. Thank you, Chairmen Hurd and Ratcliffe, Members Kelly and Richmond. My colleague from the State Department described well the background and purposes of the Wassenaar Arrangement. The U.S. Department of State leads the U.S. delegation to the Wassenaar Arrangement. But it is my agency, the Commerce Department's Bureau of Industry and Security, which is responsible for developing and administering the set of regulations, the Export Administration regulations that would implement the multilateral agreements that were just described. And in this case, the Wassenaar Arrangement for us pertains to dual-use items and some military items on the Wassenaar list.

Other agencies, primarily the Department of Defense, participates in developing proposed changes to these lists, proposed controls to submit to the Wassenaar and other arrangements, deciding which ones to agree upon, and then review the regulations that we would implement to implement the agreement. And then Congress also has technical advisory committees that work with us on reviewing the proposed changes and proposals to be submitted to the various regimes.

In December of 2013, the Wassenaar Arrangement approved new export controls on command and delivery platforms for intrusion software and related technology. Specifically, the entries in category 4 dealing with computers of the dual-use control list would control non-publicly available software that generates, operates, delivers, or communicates with intrusion software. And an intrusion software was defined as software designed to covertly gain access to a computer or other network device and, once inside, to extract or modify data or modify an execution path of the device to allow the execution of externally provided instructions.

Related hardware and technology entries would control systems and equipment for generating, operating, delivering, or communicating with this intrusion software. And then, also, technology for developing the intrusion software was controlled as well.

The original proposal for these controls came from another Wassenaar member in 2012. And the examples of the types of commercial hacking software intended to be captured by the control included those offered by Hacking Team from Italy, Gamma/FinFisher from Germany, and Vupen in France.

The controls were novel in that they were the first foray by a multilateral regime into the area of offensive cyber tools. The agreed-upon entries covering software intentionally excluded intrusion software itself from control, that is, certain kinds of malware, because of a general understanding that everyone with a mobile device might have such software unwittingly on their device and didn't want to expose them to perpetual liability. In beginning, however, the process at Commerce of drafting the regulation to implement the control, we grew concerned that despite several exclusions set forth in the definition of intrusion software, the scope of the controls, particularly the developmental technology controls,

might be far broader in scope than originally understood by Commerce and its advisory committees.

We particularly became concerned that the category 4 technology control list entry in the draft regulation technology for the development of intrusion software could inadvertently significantly harm both U.S. Government and U.S. private sector cybersecurity programs and efforts if implemented.

So in order to not take action that would inadvertently harm our Nation's ability to engage in critical cyber defense and related research work, we decided, in May of 2015, to take the unprecedented step of publishing these Wassenaar control list entries as a proposed rule with a request for private sector comments, rather than our usual step of publishing it as a final rule.

Our hope was that the private sector comments would give us a better sense for whether the rule would have unintended impacts on our cyber defense and cyber research ecosystems. All dual-use controls have consequences and impose cost on the private sector. That's the nature of controls. But this one was different because the impact would not just be on the economic bottom line of a company, but on our Government's and our Nation's ability to share efficiently and quickly the types of technology necessary to conduct cyber defense and related research.

Also, immediately following the publication of the proposed rule, we received questions from U.S. private sector and others in the U.S. Government about the intended scope of the controls. And in order to make sure that we addressed all of their concerns, we published a series of FAQs. As will be described later by our industry panelists and as is described in more detail in my testimony, we received over 260 comments, generally, all of them negative, describing several concerns that you've all summarized well in your opening statements.

I want to make clear that the administration has not made any decisions regarding what the next step will be other than that the next step will not be a final rule. We're continuing to review the comments. We're continuing to work with our colleagues in government and industry with expertise in equities and cyber defense and related research. We welcome all views and all information, which is why we thank you for this hearing and whatever input or suggestions or advice that you have for us. So thank you very much.

[Prepared statement of Mr. Wolf follows:]

Statement of

Kevin J. Wolf
Assistant Secretary of Commerce for Export Administration

Before the

House Committee on Oversight and Government Reform
Subcommittee on Information Technology

And the

House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

January 12, 2016

Thank you, Chairmen Hurd and Ratcliffe, and Ranking Members Kelly and Richmond.

The Wassenaar Arrangement is a 41-member export control group in which the United States participates. It was established to contribute to regional and international security and stability by promoting greater responsibility in the transfer of conventional arms and dual-use goods and technologies, thus preventing destabilizing accumulations of such items. Participating States maintain a common control list of items warranting control for these reasons and seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities that undermine these goals, and are not diverted to support such capabilities. The list of such items is developed and updated by the Participating States through consensus determinations, generally made at the end of each year.

The U.S. Department of State leads the U.S. delegation to the Wassenaar Arrangement but my agency, the Department of Commerce's Bureau of Industry and Security, is responsible for developing and administering the U.S. regulations – the Export Administration Regulations – that implement U.S. export controls for dual-use and some military items on the Wassenaar control list. Other agencies, primarily the Department of Defense, participate in developing proposed changes to the control list to submit to Wassenaar, deciding whether and which controls to agree to, and reviewing the U.S. regulations to implement controls agreed to by the member states. Commerce also has technical advisory committees composed of private sector experts who provide technical and other advice regarding proposals to the regimes.

In December 2013, Wassenaar approved new export controls on "command and delivery platforms" for "intrusion software" and related technology. Specifically, the entries in Category 4 (Computers) of the Wassenaar dual-use control list would control non-publicly available software (4.D.4.) that generates, operates, delivers, or communicates with "intrusion software." "Intrusion software" is defined as software designed to covertly gain access to a computer or other networked device and, once inside, to extract or modify data or modify the execution

path of the device to allow the execution of externally provided instructions. Related hardware and technology entries (4.A.5. and 4.E.1.c.) control systems and equipment for generating, operating, delivering, or communication with "intrusion software," and technology for developing "intrusion software." The original proposal for these controls came from another Wassenaar member nation in 2012. Examples of the types of commercial hacking software intended to be captured by this control include those offered by Hacking Team (Italy), Gamma/Fin-Fisher (Germany), and Vupen (France).

The controls were novel in that they were the first foray by a multilateral export control community into the area of offensive cyber tools. The agreed-upon entries covering software intentionally excluded "intrusion software" itself -- that is, certain kinds of malware -- from control because of a general understanding that everyone with a computer or mobile device infected by such malware or "exploits" could become an unwitting "exporter" of it (e.g., by forwarding an infected e-mail to someone in another country). The technology entry, however, imposes controls on non-publicly available technology for the development of such software as well as on technology for the development of the controlled delivery systems.

In beginning the process of drafting the regulation to implement the control, Commerce grew concerned that, despite several exclusions set forth in the definition of "intrusion software," the scope of the controls, particularly the technology controls, might be far broader in scope than originally understood by Commerce and its advisory committees. We particularly became concerned that the Category 4 technology control list entry in the draft regulation -- technology for the development of "intrusion software" -- could inadvertently significantly harm both U.S. government and U.S. private sector cybersecurity programs and efforts if implemented.

In order to not take an action that would inadvertently harm our nation's ability to engage in critical cyber defense and related research work, we decided in May 2015 to take the unprecedented step of publishing these Wassenaar control list entries as a proposed rule, with a request for private sector comments, rather than as a final rule. Our hope was that the private sector comments would give us a better sense for whether the rule would have unintended impacts on our cyber defense and cyber research ecosystems. All dual-use controls have consequences and impose costs on the private sector. That is the nature of controls. This one, however, was different because the impact would be not just on the economic bottom-line of U.S. companies, but on our government's and our nation's ability to share efficiently and quickly the types of technology necessary to conduct cyber defense and related research.

Immediately following publication of the proposed rule, Commerce received questions from U.S. private sector and others in the U.S. Government about the intended scope of the controls. In order to ensure that comments were informed and responsive to the proposed controls set forth in the rule, Commerce published answers to a list of "frequently asked questions" on its website to address what we determined were regular queries in order to encourage more focused and more useful public comments. It was clear from these initial questions that the terminology used in the control list entries and the proposed rule were understood differently by the cybersecurity community than by the export control agencies and the Wassenaar Participating States. By the end of the 60-day comment period, Commerce

had received more than 260 comments, virtually all of them negative. Some commenters took the view that the underlying control at Wassenaar could not be implemented without causing significant harms to cybersecurity. Others made specific recommendations on ways to mitigate many of the concerns. Some praised the underlying objectives of the rule, while nonetheless proposing modifications to the scope of the proposed regulation, such as through license exceptions and definitions, to reduce the impact of unintended consequences.

The negative reactions were repeated by extensive outreach our bureau conducted with the security industry, information security and financial institutions, and government agencies that manage cybersecurity. Outreach included multiple open meetings under the auspices of Commerce's technical advisory committees and extensive discussions with cybersecurity managers in the Federal Government.

Neither the Commerce Department nor the Administration has reached a conclusion about how to respond to the public comments. We are still reviewing and considering them. Importantly, all U.S. Government agencies with expertise and equities in cyber defense research and related work are reviewing the comments and will provide input as a next step, before we make a decision on what to do about the proposed rule. As requested by your committees, I can, however, summarize the essence of the comments – reiterating that the Administration has not come to any final conclusions regarding how to respond to the comments or to the extent to which they are correct technically. The public comments, including presentations at technical advisory committee meetings during the past three months, focus on three main issues.

First, some commenters asserted that the proposed regulation's definition of "intrusion software" is too broad and, as a technical matter, fails. They assert that malware recovery tools would be caught by the entries because they interact with malware to regain control of an infected system, and some defense research tools would be caught because they analyze malware to develop new defensive products. They also assert that products that patch systems or add capabilities to programs would themselves be controlled under these entries because of the way they interact with or manipulate programs. These products are integrated with the hardware (systems, equipment, and components) and are designed to legitimately bypass or defeat protections, modify the standard execution path of software, and access data. According to the commenters, they would often thus be software for the generation, operation, delivery of or communication with "intrusion software" and caught by the new controls.

Second, other commenters contend that the proposed rule to implement the control list entries as written, based on the definition of "intrusion software," would impose a heavy and unnecessary licensing burden on legitimate transactions that contribute to cyber security. Government agencies and private sector cyber security companies routinely test their systems and networks to identify vulnerabilities and, if possible, discover existing malicious attack agents. These companies then provide their clients with threat mitigation tools and strategies. To accomplish this, they use the same tools the controls on intrusion items identify, though their use is authorized by their target. To accomplish their mission, they need to employ tools for computers or networks that have the functional specifications of the control parameters, *e.g.,* avoid detection, defeat protective countermeasures, extract data or information, modify

system or user data, and modify the standard execution part of a program or process to execute externally provided instructions. These are exactly the characteristics a successful malicious attacker's software would have and what the assessment team's tools need to be able to replicate. During these defensive engagements, members of the assessment team frequently need to create custom scripts (i.e., software programs) to effectively assess the extent of the vulnerabilities by creating exploits, and to determine if a successful attack has taken place or is in progress.

Third, other commenters state that the proposed rule's controls on technology for the development of "intrusion software" could cripple legitimate cybersecurity research. To address cyber threats, technical information must be shared with experts across the globe. In order to identify and quickly counter threats, the cybersecurity industry relies heavily on collaboration with other companies within and outside of the United States, as well as independent experts around the world. Many of these experts are self-taught, have no prior formal relationship with cybersecurity firms, and, in many cases, may be unknown until they discover a new vulnerability. To address a vulnerability, a company must be able to engage in a back-and-forth dialogue with these researchers and experts. Often, the dialogue must include detailed discussion of exactly how a particular vulnerability could be exploited to gain control of a computer; without such discussion it is not possible to evaluate the risk posed by a vulnerability or to fashion an effective and comprehensive defense. Some commenters were concerned that, by subjecting vulnerability research, assessments, and testing to export licensing requirements including classification, screening, and other control elements, the control would limit the ability to fix and patch such vulnerabilities, leading to an overall decrease in the quality of cybersecurity. When vulnerabilities are discovered, they must be reported as soon as possible so that a fix can be developed. This process involves sharing not only the vulnerability and exploit, but also the technical information on how the exploits work, including the technology to develop them.

The commenters had many suggestions regarding how to address their concerns. The Administration will be reviewing all of them and many other ideas for how to address the policy objectives of the control but without unintended collateral harms. As I have said many times in response to questions about the rule, the only thing that is certain about the next step is that we will not be implementing as final the rule that was proposed. In working through this process, we will continue to seek input from those with expertise and equities in cyber security in both the U.S. government and the private sector before deciding in conjunction with its interagency partners what the next step should be. I thus welcome the Subcommittees' inputs and am prepared to answer any questions you may have.

Mr. RATCLIFFE. Thank you, Mr. Wolf. Dr. Schneck, you're recognized for 5 minutes.

STATEMENT OF PHYLLIS SCHNECK

Ms. SCHNECK. Thank you. Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, Ranking Member Richmond, and members of these committees, thank you for the opportunity to testify today. And thank you as well for all the support that all of your committee continue to provide to the Department of Homeland Security, most recently in the Cybersecurity Act of 2015, which was discussed earlier. Because of that legislation, we will be able to, at the Department, with our industry partners, with our interagency partners, and global partners, share cyber threat information more rapidly, and in near real time.

We appreciate the critical part that export controls play in ensuring that bad-intentioned people do not get their hands on good technology to hurt others. We also appreciate the concerns expressed by our partners and mentioned in previous testimony that show how some of these controls that are talked about today can actually potentially hurt cybersecurity efforts.

So based on these concerns raised by industry and the potential impact on the Nation's cybersecurity, the Department of Homeland Security believes that the interagency together should reexamine the merits of the proposed rule. DHS plays an increasing role in cyber and in export control. And we seek a balance between getting to that right place in protecting dual-use technology, and also incorporating the best expertise globally and protecting our cyber infrastructure from the very rapid change that we see and the sophistication of the actors of which I and others have testified before you.

In my experience, before the 2-plus years I've spent at the Department, I was in private industry. I experienced product design. I experienced research. I experienced threat dissemination and sharing with both other private sector colleagues and companies, as well as our interagency partners in government, as well as around the world. That is the best thing that we can do to protect our cyber infrastructures is, as the Cybersecurity Act that you just gave us allows us to do, put threat pictures together, put indicators together, work with the smart people around the world at the speed of light, in the speed of cybersecurity that our adversaries are operating in.

We hear a lot about the Internet of things. That means that almost anything you can see and touch has a computer processor in it in the future. That means that all those things are exposed to cybersecurity vulnerabilities. And that means we need the power of speed to put that story together, to disseminate it rapidly, to share research, and design products that protect better. We need the collaboration.

In this environment, researchers and developers need to be able to work together with alacrity. They need that in the government. We need it in the private sector. And we need to be able to work together at the very speed and hopefully greater than that speed at which our adversaries are working today. A good example of how

the Department works was in the Heartbleed episode in April, 2 years ago. The Department of Homeland Security received information from another government that there was a vulnerability in an open source encryption algorithm, as you well know. We were able to, through our United States Computer Emergency Response Team, disseminate that information internationally. Our CERT works, that's the Computer Emergency Response Team, our CERT works with over 300 different CERTs internationally to get that information out there.

Our cybersecurity companies and our private sector are global. Our government needs to work with other governments. The U.S. has taken a leadership role because of our ability to share and collaborate and push cybersecurity and cyber threat information out as far as we can. And companies and governments need these tools and need to be enabled to have the same alacrity with which our adversaries are enabled.

Our adversary works, as I mentioned before, without lawyers. They have plenty of money. They have no boundaries. And as was mentioned earlier, we want to bypass jurisdictional roadblocks. We thank you for that. We in cybersecurity need to bypass competitive roadblocks. We need to bypass time roadblocks. And we need to be able to collaborate, again, without interruption.

Cybersecurity is a joint effort, involving government, private sector, and academia. We welcome the chance to work together, our three agencies, our entire administration, the interagency, with all of our government partners to ensure, again, our global leadership in cybersecurity, our global ability to share this threat information. This is the main thing our adversaries cannot do. This is the product set that our companies can build for us. This is the ability for us as a government to leverage all that innovation in the private sector and push it forward.

And our position is we would like to, as an interagency together, reexamine the merits of that rule by striking a very good balance, getting it right, ensuring that we have all the benefits of the hard work that's done in export control, but also ensuring that cybersecurity doesn't stop. Anything we do to delay the collaboration between any smart mind that we can find, human or machine, enables our adversary. So thank you. And I look forward to your questions.

[Prepared statement of Ms. Schneck follows:]

Testimony of

Dr. Phyllis Schneck
Deputy Under Secretary for Cybersecurity and Communications
National Protection and Programs Directorate
United States Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
And the
Committee on Homeland Security

January 12, 2016

Introduction

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, and Ranking Member Richmond and distinguished members of the Committees, let me begin by thanking you for the unwavering support provided to the Department of Homeland Security (DHS) and the National Protection and Programs Directorate (NPPD). We look forward to continuing to work with you in the coming year to ensure a homeland that is safe, secure, and resilient against terrorism, cyber-attacks, natural disasters, and other risks.

In particular, we appreciate Congress' efforts in passing the Cybersecurity Act of 2015 last month. This invaluable legislation will significantly enhance our ability to exchange cybersecurity threat information between the government and the private sector and will improve our ability to protect federal civilian networks.

NPPD undertakes its cybersecurity activities within its overarching mission to secure and enhance the resilience of the Nation's cyber and physical infrastructure. We view ourselves as a customer service organization, and our customers are federal civilian departments and agencies, state, local, tribal, and territorial governments, and the private sector. NPPD strives to

understand the mission, interests and equities of all of our customers to build trusted relationships for knowledge exchange and to better enable their resilience by creating and offering the right services and capabilities.

Within the private sector, NPPD maintains a particularly close partnership with the cybersecurity community – developers, vendors, and researchers that create the innovative solutions to help protect our Nation from cybersecurity risk. It is in this context that we consider the 2013 Wassenaar Agreement on Intrusion and Surveillance Items. I appreciate the concerns raised by many Members of Congress.

By way of background, the Wassenaar Arrangement (WA) on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multi-lateral forum intended to promote transparency and greater responsibility with regard to transfers of conventional arms and dual-use goods and technologies. In 2013, Participating States to the WA agreed upon a new export control for ''systems,'' ''equipment,'' or ''components'' thereof, ''specially designed'' or modified for the generation, operation or delivery of, or communication with, ''Intrusion Software.'' Pursuant to this unanimous agreement, the Department of Commerce engaged in a rulemaking process as the U.S. Government's lead for domestic implementation of WA rules. Industry feedback to a Notice of Proposed Rulemaking (NPRM) was overwhelmingly negative and raised significant concerns regarding implications for cybersecurity innovation, research, and information sharing.

NPPD and the DHS Science and Technology Directorate, the Department's export control lead, have further consulted with numerous industry groups and solicited feedback through the Sector Coordinating Councils. For context, Sector Coordinating Councils are structures of the National Infrastructure Protection Plan Framework that bring together executives in the private sector to collaborate with each other and with the U.S. Government on key issues of cyber and infrastructure protection, transcending the competitive boundaries that traditionally block this type of collaboration within a sector. Most of our critical infrastructure sectors have a Sector Coordinating Council. It is important to note that the private sector participants expend great energy, resources and intellectual capital in these Sector Coordinating Councils, because they

know that the government strongly considers the resulting sector views in future planning and policymaking.

DHS understands that there are national security concerns that led to the development of this control with the aim to restrict exports of such tools related to intrusion software so they cannot be used maliciously. However, we need to ensure that in implementing the 2013 control, the U.S. does not inadvertently create greater problems and more risks than the security concerns that the control was intended to address. The interagency, including DHS, shall consider carefully the concerns raised by U.S. industry and legitimate potential impacts on the Nation's cybersecurity.

As the Committee knows, cybersecurity is defined by rapid change. Technology is evolving at a faster pace than ever before. Our adversaries are also changing rapidly, and are constantly developing new tools and attacks to compromise critical networks, steal data, and potentially damage our physical infrastructure. In this environment, it is essential for cybersecurity researchers and developers to share information rapidly across borders in the interest of creating the next security solution or combating an emerging risk.

For example, national cybersecurity response teams (such as Computer Security Incident Response Teams (CSIRTs)) rely on timely and actionable information about cybersecurity threats and vulnerabilities from researchers and other independent experts. In the United States, our CSIRT resides within NPPD, and is called the United States Computer Emergency Readiness Team (US-CERT). US-CERT relies upon international counterparts on a daily basis to help identify, respond to, and mitigate cybersecurity risks that threaten government and critical infrastructure networks. A substantial portion of information sharing with cybersecurity researchers occurs across national borders and this needs to be taken into account in implementing export controls.

Finally, there is a critical need for increased and sustained investment in cybersecurity research and development, rather than less. In crafting our approach to implementing the Wassenaar control, we need to take this intro account, as well as the uncertainty expressed by many cybersecurity firms regarding the specific types of information that can be shared with their foreign-based subsidiaries, or with their own foreign national employees within the United States, without a license.

Evolving and sophisticated cyber threats pose a considerable challenge to securing critical infrastructure and government systems. As such, governments should implement policies to incentivize innovative research in measurably effective cybersecurity.

The United States is fortunate to have many global leaders in cybersecurity research and innovation within our borders. We also need to ensure that implementation of the Wassenaar control does not unduly disadvantage these companies in a global competition with their international peers.

Of course, NPPD is fully conscious of the significant risks posed by certain surveillance tools and intrusion software. There are myriad examples of governments using such tools to spy on dissidents, constrain freedom of expression, and engage in extrajudicial monitoring. But such examples also exemplify why we must support improved cybersecurity. We need a balanced approach that both protects cybersecurity research and innovation and make it harder for authoritarian governments to monitor dissidents or for cyber criminals to steal data about U.S. citizens. The inherent nature of many "cyber technologies" is that they are technologically agnostic; that is, the same software that is used to test a company's cybersecurity can be used to conduct unauthorized or illegal surveillance. This demonstrates the complexity of the issue, and why further discussion is needed.

The Wassenaar Agreement on Intrusion and Surveillance Items was developed in response to a legitimate concern: reducing the proliferation of dual-use technologies that are used for malicious surveillance or hacking. But in implementing that control we need to avoid unintended consequences on cybersecurity. In a threat environment where our adversaries continue to gain in sophistication, we cannot afford to unduly constrain development of the next generation of cybersecurity solutions. Cybersecurity developers and vendors must be able to share information for legitimate purposes as quickly as possible. Researchers must be able to share apporopriately vulnerability and threat information with US-CERT and national CSIRTs in friendly states. The interagency continues to consider the issue. In the meantime, DHS will continue to support national security efforts undertaken at the Wassenaar Arrangement while continuing to work with our interagency partners to strengthen U.S. cybersecurity.

Mr. RATCLIFFE. Thank you, Dr. Schneck. The chair now recognizes Ms. McGuire for her opening statement.

STATEMENT OF CHERI F. MCGUIRE

Ms. MCGUIRE. Chairman Ratcliffe, Chairman Hurd, Ranking Member Kelly, and Chairman Thompson, other distinguished members of the committee, thank you for the opportunity to testify today on behalf of Symantec Corporation. This hearing is extremely timely. And we very much appreciate your shining a spotlight on a vital issue that threatens the cybersecurity of not only the U.S. technology industry, but also that of all U.S. critical infrastructure companies and organizations that rely on cybersecurity.

The proposed U.S. cybersecurity export regulation under the Wassenaar Arrangement would severely damage our ability to innovate and develop new cybersecurity product, conduct real-time global research, and share information on vulnerabilities and exploits, as well as to test and secure global networks and new technology products.

These new regulations would restrict the free flow of information across borders and impose major new export compliance burdens on all U.S. multinational industries. While the regulation grew out of well-intended concerns over the availability of intrusion and surveillance software to repressive regimes, the end result has swept in the core functionality of cybersecurity products and technology, and puts untenable restrictions on security testing and research.

The fact is, this is not an export control on a few specific tools. It is a stringent new regulation on the entire cybersecurity industry, and our customers that would harm the economic and national security of the United States. Ultimately, it would leave every American less protected and vulnerable to cyber criminals and cyber terrorists.

The regulations would capture many common and critical security tools. One of these is penetration testing. These tests are designed to stress systems just as real attackers would and expose weaknesses that would allow an organization to improve its defenses. Yet, under the proposed regulations, financial services, health care, energy, and other multinational companies would need export licenses merely to do security testing on their overseas systems and products.

We have other concerns, but I feel compelled that I need to raise one more. As you all know, Congress and the administration have just acted to improve cyber threat information sharing. Yet, these regulations would undo much of that effort. As many of you have said today, cybersecurity knows no borders. But at Symantec, in our business practices, we also operate security operations centers around the world. Under these regulations, we would be required to apply for and wait for an export license before discussing much of our security research with a U.S. citizen who was working in one of our international centers. And the underlying rule does not even envision the accommodation of real-time machine-to-machine information sharing across borders.

As we all know, cyber threats move at light speed, not bureaucratic speed. And as Chairman Hurd said, the clock starts ticking when an indicator of compromise is identified.

To provide some perspective, Symantec's intrusion prevention systems blocked approximately 300 million exploit kits for our global customers in 2015, one of the exact technologies that would be restricted under this rule. Companies like ours rely on unfettered research and communication to innovate and develop the next generation of security technologies. At Symantec, our preliminary assessment showed we would need at least 1,000 new licenses. Today, we need less than a dozen. But the truth is that we've stopped counting, as the number is likely to go even higher. Coupled with an average lead time of 6 months to develop a license application, there is no doubt that these new burdens would cripple our ability to respond to real-time threats and cyber attacks.

Another issue is that countries that are party to the Wassenaar Arrangement and have implemented the rule have taken vastly different approaches. There are multiple interpretations of the underlying language that have led to confusion, and implementation differs significantly from country to country. In fact, today, we at Symantec are holding up a product released in one country, while our lawyers try to figure out the next steps that should be taken. And we've seen other U.S. companies who are already pulling back on international research engagements because their attorneys say there is too much risk for cross-border research flows.

The simple fact is that the rule will do little to stop the spread of malicious intrusion and surveillance tools, or curtail illicit hacking and intrusions in any way. In fact, the current rule would do just the opposite. It would handcuff security vendors and multinational companies from using all the tools available to them, while imposing no restrictions on cyber criminals. After hearing significant concerns, the Department of Commerce, to its credit, quickly withdrew the proposed rule. The conversations that have followed have been extensive and frank, but, ultimately, unsuccessful. This is not because of a lack of good faith on either side, but because of defects routed in the 2013 Wassenaar cybersecurity agreement.

For this reason, we strongly recommend that the rule be remanded back to Wassenaar to be renegotiated and more narrowly defined. Of course, we look forward to continuing to work with Congress and our U.S. Government partners, to share our technical expertise on this very important issue to our industry and critical infrastructure in the U.S. Thank you for the opportunity to testify today. And I look forward to any questions you might have.

[Prepared statement of Ms. McGuire follows:]

Chairman Ratcliffe, Chairman Hurd, Ranking Members Kelly and Richmond, and distinguished members of the Committees, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda and government engagement strategy, and represent the company in key public policy initiatives and partnerships. Currently I serve on the World Economic Forum Global Agenda Council on Cybersecurity, and on the boards of the George Washington University Center for Cyber and Homeland Security, the Information Technology Industry Council, and the National Cyber Security Alliance. From 2010 to 2012 I served as the Chair of the U.S. IT Sector Coordinating Council – one of 16 critical infrastructure sectors identified by the President and the U.S. Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. Previously, I served in various positions at DHS, including as head of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec protects much of the world's information, and is the largest security software company in the world, with 33 years of experience developing computer security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services (Symantec for enterprises and Norton for consumers and small businesses) protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of hundreds of millions of attack sensors recording thousands of events per second, and more than 500 dedicated security engineers and analysts. We maintain nine Security Response Centers and six Security Operations Centers around the globe. Every day we scan 30 percent of the world's enterprise email traffic, and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts and our security technologies a unique view of the entire Internet threat landscape; which in turn we use to protect our customers' most sensitive data and systems around the world.

Introduction

The hearing you are holding today is extremely timely. It shines a spotlight on a critical issue that threatens the cybersecurity of not only the U.S. technology industry, but also that of all U.S. critical infrastructure companies and organizations that operate or connect to networks overseas. The proposed U.S. cybersecurity export control rule under the Wassenaar Arrangement would severely damage our ability to innovate and develop new cybersecurity products, to conduct real time global research and share information on software vulnerabilities and exploits, and to test and secure global networks and new technology products.

These restrictions would devastate the U.S. cybersecurity industry itself and harm the security of nearly every U.S. multinational company. This rule is not an export control on a few specific tools. It is a stringent new regulation on the entire cybersecurity industry and its customers that would harm the economic and national security of the U.S. Ultimately, it would leave every American less protected against cybercriminals and cyber terrorists.

Industry and academia in the U.S. are at the forefront of designing, testing and developing some of the world's leading cybersecurity technologies. Companies like Symantec rely on unfettered research and communication to innovate and develop the next generation of security technologies. These new regulations would restrict this free-flow of information and impose major new export compliance burdens on all U.S. multinational industries. It would have three significant negative impacts on cybersecurity:

- First, cybersecurity research would be curtailed, as the rule hinders developers and researchers from testing products and networks and sharing technical information about new vulnerabilities and exploits across borders.
- Second, the availability of critical cybersecurity tools would be constrained, as the rule restricts the export of cybersecurity technologies, even to subsidiaries of U.S. companies overseas.
- Third, cybersecurity collaboration and information sharing would be harmed, as the rule deems information to be "exported" once it is shared with non-U.S. persons, even if they physically work for a company here in the U.S.

The significant time and effort that both the government and the private sector have spent jointly searching for a way to redraft the rules has not borne fruit, but not because of a lack of good faith on both sides. The effort has failed because the proposed rule contains unresolvable ambiguities and fundamental flaws – defects that are rooted in the faulty original 2013 Wassenaar cybersecurity agreement. For this reason, the U.S. redrafting effort should be suspended. The U.S. government should take a leadership role and return to Wassenaar in the upcoming plenary session with a proposal to renegotiate the original 2013 cybersecurity agreement.

In my testimony today, I will discuss:

- An overview of the Wassenaar Arrangement and the "cybersecurity rule";
- Consequences for cybersecurity tools, testing, research and information sharing;
- Other critical infrastructure sectors affected by the rule;
- Economic impacts of the rule for industry and the government;
- How other Wassenaar nations are implementing the rule; and
- Why the U.S. proposed rule is unworkable, and solutions outside of Wassenaar.

I. Overview of the Wassenaar Arrangement and the "Cybersecurity Rule"

The Wassenaar Arrangement is a multilateral export control agreement with 41 nations as signatories that was designed to cover conventional arms and dual-use goods and technologies and prevent proliferation of sensitive components. It did not originally envision, nor was it designed for, widely available cybersecurity software technologies. There is a process for adding new controls, and under the 2013 agreement, the United Kingdom offered a proposal that "intrusion" and "surveillance" software be added to the list of export-controlled technologies. This grew out of well-intended concerns over the availability of "intrusion software" to abusive regimes and the need to protect dissidents. As the control was being developed, we are not of aware of any consultations with the U.S. cybersecurity industry about its real world implications, given that the underlying software functionality of intrusion software is the same or similar to other widely used security technologies.

Though the Wassenaar Arrangement is non-binding, it has long been the policy of the U.S. to fully implement agreements under it and to update its own export control regime accordingly. As part of the U.S. implementation of this new control, in May 2015 the Department of Commerce (DoC) published for comment in the Federal Register a proposed amendment to the U.S. export regulations that would cover cybersecurity products categorized as "intrusion and surveillance items." Due to the overly broad definitions in the Wassenaar control and the subsequent U.S. rule, industry and academia submitted an unprecedented volume of approximately 300 formal comments, nearly all of them strongly objecting to the new regulations.

Symantec, like many others, demonstrated that the rules were written far too broadly and hindered legitimate, widely used and beneficial cybersecurity technologies and practices, including penetration testing software, white-hat research, and cyber threat information sharing. Since the initial comment

period, the DoC has proactively engaged in an impressive amount of outreach to solicit advice and input on how they could implement the rule in a way that would not severely damage U.S. economic and national security.

However, the underlying language negotiated at the 2013 Wassenaar Arrangement Plenary was so deeply flawed that, despite months of consultation, we still cannot envision language that would mitigate the numerous detrimental effects. The core problem is that the needed changes do not concern technical definitions or product lists, but instead are an issue of the user's intent when deploying widely available cybersecurity technologies. Unfortunately, the Department of State, as the lead U.S. negotiator at Wassenaar, has repeatedly rebuffed industry concerns on this point, saying the *intent* issue is not up for debate. As such, we see no other alternative than for the U.S. government to return to Wassenaar and renegotiate the underlying and overly broad control that was agreed to in 2013.

It is important to recognize however that Congress understood the importance of this issue from the start, with some of you even submitting your strong concerns through the formal DoC rulemaking process back in July. Moreover, Symantec wishes to thank many of you here today for your leadership in sending a letter last month to the President's National Security Advisor urging the Administration to send the export control rule back to Wassenaar to be renegotiated or heavily revised.[1] Spearheaded by Congressional Cyber Security Caucus Co-chairs Michael McCaul (R-TX) and Jim Langevin (D-RI), the bipartisan letter was signed by 125 Members of Congress and rightly recognizes that the proposed cybersecurity export control regulations will have a chilling effect on research and innovation, as well as negatively impact the overall cybersecurity posture of the U.S.

II. Consequences for Cybersecurity Tools, Testing, Research and Information Sharing

To understand how the proposed rule will harm cybersecurity, it is necessary to understand how common security products and tools work, the technology they are based on, and how the information generated by them is used. Symantec and the larger cybersecurity industry have serious concerns with the ambiguous and overbroad language used in the proposed rule. That language would capture not only cybersecurity products, but also basic software development and security techniques.

Of note, the rule does not specifically control actual "intrusion" software, reportedly so as not to cause victims of cyber hacking whose electronic devices may be carrying intrusion software without their knowledge to commit inadvertent export control violations. Since "intrusion" software is not itself controlled, proponents and the DoC have said the transfer of exploit samples, proofs of concept, and other forms of malware are not controlled. In reality, however, the controlling systems and technology designed to operate, deliver, and communicate with the "intrusion" software effectively sweeps the entire cybersecurity industry – including all penetration testing systems and virtually all other cybersecurity products such as anti-virus software – into the controls.

Unfortunately, it is not possible to effectively share vulnerabilities and exploits for defensive purposes, or to use defensive "intrusion software," without using control and delivery platforms and sharing the equipment, software, and/or technology behind them. While there is ostensibly no direct control of "intrusion software" itself, as a practical matter, the controls are broad enough to effectively control intrusion software by controlling items that generate, operate, deliver or communicate with it, and technology for the development, production, or use of such items. In other words, it is impossible to separate out security software common functionality. Thus, most security technologies end up being swept in for categorical inclusion.

[1] https://langevin.house.gov/sites/langevin.house.gov/files/documents/12-16-15_Langevin-McCaul_Wassenaar_Letter.pdf

Vulnerability Testing and Patching

Vulnerability testing and patching are examples of how the proposed U.S. rule would put controls on legitimate intrusion software. The DoC has stated that vulnerability scanners, which find potential vulnerabilities in a system without actually exploiting them and extracting data, would not be controlled. But this ignores the reality of the process of vulnerability research, which is not just about finding potential vulnerabilities or even sharing proofs of concept. When finding vulnerabilities and reporting them, the most valuable information is often about how the vulnerability can be exploited and how those exploits work, including the technology used to develop them. This information helps the vendor understand the root cause of the vulnerability and develop a more complete and long-lasting defense instead of just a "band aid" fix. The DoC states that it recognizes that controlled "technology" may be transferred during the reporting of a vulnerability or exploit, highlighting that this process will indeed be subject to these highly restrictive controls. The DoC also recognizes that the tools used to test vulnerabilities (which find vulnerabilities and extract data to prove the vulnerability exists) would also meet the technical description of items that fall within the control list.

Penetration Testing

Controls under the proposed U.S. rule would capture another common and critical set of tools and technology known as penetration testing (often referred to as "pen testing"). Penetration testing is a suite of tests designed to stress the target system (as real attackers would) in its operating environment. It is also used to evaluate the security of a system or software product by analyzing its weaknesses and attempting to compromise it. The testing is best done in a highly controlled environment using specialized computer systems and as part of a broader security testing strategy.

At commercial companies, typically there are two primary categories of penetration testing:

(1) Pre-production penetration testing which is done on products or a family of products before they are released for sale to customers; and

(2) Post-production penetration testing where testers operate on a much broader scope and ensure corporate networks and systems are secure.

In pre-production penetration testing, there are usually three types of tests: black-box, white-box, and gray-box. In a black-box assessment, the testers have no information prior to the start of testing. In a white-box assessment, they will have complete details of the network and applications. For gray-box assessments, the testers will have some details of the target systems. Symantec typically performs gray-box assessments on its own products, as this type of assessment yields more accurate results and provides a more comprehensive test of the security posture of the environment than does a black-box assessment.

In post-production penetration testing, testers take a much broader look into their targeted systems and approach to penetration. This process is, at all times, carefully managed, scoped, and monitored so that any dangerous vulnerabilities discovered are strictly guarded and not allowed outside of the network – or into the "wild". While this testing is directed at the target company's internal networks and systems, often times vulnerabilities in third party hardware and software used in the target's IT environment are also discovered. When these vulnerabilities are discovered, the testers must notify the developer of the vulnerable product and work with them to develop an effective remediation. All data collected, vulnerabilities found, exploits researched and developed, and remediation fixes and approaches are kept strictly within a protected environment for complete safety.

Third Party Software Updates and Patching

Similarly, third parties often engineer "exploits" to provide update services and manual patching for commonly-used software products manufactured by other companies. Such third party participation is necessary to supplement the features offered by the original provider, or where that original provider has gone out of business or has stopped supporting its code, as is often the case with critical infrastructure. Thus, not all exploits are malicious. Unlike auto-updaters that are part of the original software, these third parties use exploits to deliver updates and patches into vulnerable programs and systems. They use these exploits to defeat the integrity of the original system, bypassing its protective measures, modifying its standard execution path, and providing external instructions. Even if the "exploits" themselves are not controlled, the related controls appear to squarely capture parts of these updating and patching tools that deliver and communicate with the components that apply the security patch.

Presumption of Denial for Licenses for Rootkits and Zero Day Exploits

Another potentially negative impact of the proposed DoC implementation of the rule on the cybersecurity industry and our customers is the rule's presumption of denial for all licenses related to "rootkit" and "zero-day" exploit capabilities. In the preamble to the U.S. proposed rule, in the section titled *License Review Policy for Cybersecurity Items*, it states:

> "Note that there is a policy of presumptive denial for items that have or support rootkit or zero-day exploit capabilities."

The presumption of denial for licenses related to rootkit and zero-day exploit functionality is highly problematic. First, the policy would limit the development and delivery of defenses for the most dangerous vulnerabilities, zero-days. Zero-day vulnerabilities are previously unknown and unpatched vulnerabilities and make up the majority of what is discovered during penetration testing. In fact, many cybersecurity companies have zero-day focus groups, which specifically research these types of vulnerabilities and proactively exchange information about their exploitability with other vendors and/or manufacturers to help devise an effective defense. If zero-days are defined as vulnerabilities without a released patch, then they are the highest priority items for responsible companies to address, and it would be highly problematic if they were restricted from being shared with knowledgeable employees or outside experts, some of whom will inevitably be foreign nationals. If a company is prevented from closing a known vulnerability, the security of its customers and its own networks and products will be put at much greater risk, as cyber criminals are quick to act on these.

The presumptive denial for rootkits is similarly problematic. While the functionality of "rootkits" may vary and the term can mean different things in different contexts, a "rootkit" capability is often understood to mean simply that the item can live underneath the user interface and subvert what the user is doing without his or her knowledge. Basically, the rootkit subverts part of the operating system by interrupting it, running "underneath" it, or "hooking" into it. Then, when the operator of the system takes an action, the "rootkit" intercepts that action and modifies or subverts it without the user's knowledge so that it acts differently than as intended.

If this common definition is how the DoC interprets "rootkit" capability in the proposed rule (which is unclear since no definition is provided), any software security instrumentation framework could be seen to create a rootkit capability. Modern security modules often use "rootkit-like" functionality to integrate into the existing code of the operating system; and in doing so change the behavior of the operating system. This is known as "hooking into" an operating system. As such, a fundamental part of most security vendors' endpoint protection products are "rootkit" capabilities. For instance, when you install Symantec's Enterprise or Norton security products, they often work by hooking into the normal

operating system, monitoring the data communicated through it, intercepting and inspecting the data, and potentially changing it when it identifies a threat—all operating in the background once installed on a device. These "rootkit" capabilities are used in these products because they are the most effective means of accessing the system to monitor for and catch malicious traffic before it can fully infect the system.

"Rootkit" capabilities also are a common function of legitimate software, not just for cybersecurity. Examples include remote control software used by help desk technicians, system administration tools, technical support, and even anti-cheat mechanisms for video games. These types of software programs with "rootkit capabilities" are not malicious, but the proposed rule does not distinguish between those used with a system administrator's or user's knowledge, and those put there by a malicious actor. In light of the broad range of legitimate uses for "rootkit" capabilities, a policy of presumptive denial is clearly inappropriate and does not account for how security software is designed for interoperability.

Simply put, not every rootkit or zero-day is shared or used for malicious purposes – the cybersecurity industry uses these same exploits in order to fix dangerous vulnerabilities. Indeed, these zero-day vulnerabilities and exploits are the very items that companies seek to find and deal with in their penetration testing engagements and exercises. The inability to freely share this information and the related research and development of defenses within a company and its suppliers will severely impact the ability to create safe products and ensure a secure network and IT environment.

Further, the proposed rule will do nothing to curtail the underground market where criminals buy and sell exploits, vulnerabilities, and attack kits. What it will do is make it harder for U.S.-based organizations with operations around the world to deploy the best tools available to find the weaknesses in their own systems and to patch them – before an attacker does.

Real-Time Information Sharing

The cyber threats we face every day are growing in both numbers and sophistication. Over the last three years we have seen more than *one billion* identities exposed through breaches. Sensitive trade secrets and intellectual property are being pilfered at an unprecedented rate. As detailed in Symantec's 2015 Internet Security Threat Report, the use of malware is growing and becoming more sophisticated, with nearly *one million* new variants released every day.[2] Attackers are constantly evolving and honing their capabilities to avoid detection, and there are a broad set of tools available to them.

Vulnerabilities continue to be a big part of the security picture, where operating system and other patches have been critical to helping keep systems secure. For example, in April 2014, the discovery of vulnerabilities such as Heartbleed and ShellShock, and their widespread prevalence across multiple operating systems exposed millions of consumers and businesses worldwide to attack. These vulnerabilities existed in the underlying web authentication protocols (SSL and TLS) and given the seriousness, created a global call to action for companies, researchers and governments. Within four hours of the Heartbleed vulnerability becoming public, Symantec saw a massive surge of attacks, and cybersecurity professionals around the world mobilized to coordinate and respond.

This is the exact type of urgent and necessary global collaboration that would be impractical and severely hindered under the U.S. rule where we would be required to apply for and wait for an export license before discussing such vulnerabilities with non-U.S. nationals. Compounding the issue is that even if all parties applied for an export license to be able to share such information, that request would be presumptively denied under the current U.S. rule.

---

[2] Symantec Internet Security Threat Report, April 2015.
http://www.symantec.com/security_response/publications/threatreport.jsp

Another area that would be impacted is information sharing with global law enforcement and government agencies. Today, Symantec shares cyber threat information with international cyber response organizations and law enforcement entities around the world, including INTERPOL, EUROPOL, and national CERTs and cyber police agencies. This work often extends to specific global cybercrime cases, such as botnet eradication and criminal prosecutions.

For example, in February of 2015, Symantec and other industry players partnered with EUROPOL, the FBI and other national law enforcement agencies in an operation to disable the infrastructure controlling the *Ramnit* botnet and the criminal gang that operated it. *Ramnit* harvested banking credentials from its victims and had infected more than 3.2 million computers across the globe.[3] It is a fact that cybercriminals do not recognize national borders when they commit crimes. However, under the U.S. proposed rule, we could be required to seek a license every time we wanted to share threat information across borders with international law enforcement, severely limiting the successful public-private partnerships we have had to date.

Further, as a global cybersecurity company, Symantec has researchers, engineers and analysts in our operations centers around the world. Under the current U.S. rule, our American employees working in the U.S. would be required to first obtain a government license if they were going to engage in anything more than a cursory conversation about new security vulnerabilities or exploits with any co-worker who is either not a U.S. citizen or who is located outside the U.S. (even if that foreign-based employee was a U.S. citizen). Further, if our U.S. researchers discovered a zero-day vulnerability in one of our non-U.S. customer's products or systems, and we wanted to share that information with the customer, again we would be required to obtain an export license.

In addition, the rule does not envision the accommodation of real-time machine-to-machine information sharing across borders – a function that modern security analytics, detection and protections heavily rely on today. At a time when cyber threats are increasing, it is critical that sharing of cyber threat information – whether by humans or machines – remains unfettered. Long a priority for the Congress and the Administration and as seen in the recently enacted law, cyber threat information sharing would suffer under this export control.

The simple fact is that the rule will do little to stop the spread of malicious intrusion and surveillance tools, or curtail illicit hacking and intrusions in any way. In fact, the current rule would do just the opposite – handcuff security vendors and multinational companies from using all the tools available to them, while imposing no restrictions on cyber criminals.

III. Other Critical Infrastructure Sectors Affected by the Rule

The proposed rule would have severe impacts beyond just the cybersecurity industry as other critical infrastructure sectors and academia would also be required to obtain export licenses for the use and deployment of these tools. Certain industries are legally required to conduct penetration testing, and some have implemented this type of testing as part of their industry standards and best practices, including the financial services, electricity, and healthcare industries.

Under the proposed rule, companies using testing tools and processes to comply with regulatory requirements and industry standards for their networks or facilities outside the U.S. also will need to implement costly and time-consuming changes to their internal compliance programs to obtain export licenses. The consequences of the delays created will undermine existing industry standards and regulations, weaken security, and lead to more frequent security breaches across critical infrastructure sectors.

[3] http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation

The financial services industry has its own, unique information security requirements. A frequent target of attacks, banks perform a high level of due diligence to ensure the confidentiality, integrity and availability of customer transactions. Penetration testing is one way to stress the attack surface that an organization presents to the outside world. Under the rule, any multinational U.S. financial institution would be required to seek an export license before testing its own networks. As the Financial Services Roundtable/BITS made clear in its formal comments to the DoC, the proposed rule would "seriously diminish the financial industry's ability to effectively run day-to-day cybersecurity assurance programs."[4]

The power industry is another critical infrastructure sector that is required to conduct penetration testing. As part of the North American Electric Reliability Corporation (NERC) CIP standards, cybersecurity is recognized as a critical factor in protecting the nation's electric grid. Similarly, the healthcare industry has heightened privacy and security concerns associated with the electronic transmission of health information. The Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 strengthened civil and criminal penalties for breaches and non-compliance with HIPAA standards. By restricting the necessary cybersecurity tools to test overseas networks and products, the rule will make compliance with such requirements more difficult for U.S. multinational companies.[5]

Information sharing would also be an issue for the critical infrastructure sectors. The Financial Services ISAC and the Energy ISAC, both with successful information sharing programs among their company members, also would likely be required to obtain export licenses in order to conduct their business across borders. In addition, in the healthcare sector, one could imagine a scenario where a U.S. multinational healthcare device manufacturer discovers a life-critical, zero-day vulnerability in a product. Under the U.S. rule, the company would be prohibited from sharing details with its experts – or even its customers – around the world while it waits for weeks or months to obtain an export license. Meanwhile, the vulnerability would sit unfixed and open for attack during that time.

IV. Economic Impacts for Industry and Government

U.S. companies design, test and deploy much of the world's leading security technology. The U.S. is also home to most of the world's cybersecurity companies, holding the number one provider position in the global market – which topped $75 billion in 2015 and could reach $170 billion by 2020.[6] The proposed rule will have a disproportionate effect on the U.S. cybersecurity industry, because most of the companies are based here. In addition to the economic effects on the cybersecurity industry, the rule would also lead to less secure networks and make them easier prey for cybercriminals. While estimates vary, cybercrime experts have put the annual global cost of cybercrime at $400 billion or more.[7] Without the benefit of cutting edge research and security available to consumers and companies, this number could rise significantly.

Companies implementing the new rule will surely feel the financial impacts as significant new legal and compliance resources will be needed just to manage this one regulation. At Symantec, our preliminary assessment showed that initially we would need approximately one thousand new licenses, but the actual number could go much higher. This is in comparison to our current annual filings that number less than a dozen. Equally as important, the new regulations would require us to significantly alter our trade compliance program. These changes would result in the hiring of additional compliance personnel and a six-month lead time to collect the information necessary to submit any new export license

[4] http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0231
[5] http://www.regulations.gov/#!documentDetail;D=BIS-2015-0011-0209
[6] http://www.csoonline.com/article/2946017/security-leadership/worldwide-cybersecurity-market-sizing-and-projections.html
[7] http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf

requests. The added burdens would impede Symantec's ability to be nimble and agile in responding to real-time threats and cyber attacks.

Further, it is not clear how we would even write a license application given the fact that our penetration testing processes allow for detection of unanticipated vulnerabilities and additional follow-on testing if needed. We envision a scenario where we conduct a test, find that we need to do more or different testing, and then must stop to wait weeks or months for another export license. In the meantime, our networks could remain vulnerable, or our product development and security protection release cycles would be significantly delayed. Both of these would have substantial financial and market impacts on our business. We envisage that most other companies would incur similar economic impacts.

There are also implications for cybersecurity start-ups and small businesses who do not have the compliance programs that large companies have, or know how to deal with these rules. By placing such a heavy compliance burden on small innovators, the likely end result is that the U.S. will drive the cybersecurity industry offshore as the U.S. system will be too complex and resource intensive. When combined with a more stringent U.S. implementation than other nations, start-ups will be even more competitively disadvantaged.

On the government side, the proposed rule represents an unknown but significant licensing burden for the DoC Bureau of Industry and Security (BIS) that is responsible for managing the U.S. export control regime. The exponential increase in license applications from all industries, coupled with the enforcement needed to ensure compliance, would require significant new taxpayer resources. It is highly unlikely that the BIS, as is currently staffed, has the capacity to evaluate and process such a large volume of new applications.

V. International Implementation

Not only do the proposed Wassenaar controls damage U.S. economic and national security, but they also do not effectively control the very export of the items they are targeting. For one thing, countries that are party to the Wassenaar Arrangement and already implemented the rule have taken vastly different approaches. There are multiple interpretations of the underlying Wassenaar agreement language that have led to confusion and implementation that differs significantly from country to country. It is clear that the requirements under the Wassenaar Arrangement differ significantly from how countries are implementing the rule.

For example, in Japan, the government worked closely with industry and the Center for Information on Security Trade Controls, resulting in broad carve-outs for nearly any conceivable cyber security product, technology, and research. However, in the end and when viewed clearly, this is simply a case where a Wassenaar country has recognized that there is no way to control malicious hacking products and technology without also causing severe damage to the legitimate cybersecurity industry and its customers. Unintentionally, Japan has added to the variations on implementation of the control, which inevitability will hold up multinational companies' testing and development work.

A direct result of this ambiguity occurred last year when Hewlett-Packard (HP) and its Zero Day Initiative declined to participate in an annual hacking contest in Japan. HP's head of threat research, Jewel Timpe, cited Japan's implementation of Wassenaar as the reason, and that the risk associated with the real time transfer of research across borders could not be reconciled by their legal and compliance teams. She said, "It's due to difficulty in handling, defining and getting the licensing in real time that the contest demands. On the ground running the contest, how does one effect transfers and not run afoul of the

arrangement? There was no clear path to do that easily and quickly."[8] There is no doubt that the same questions and lack of clarity will stifle and impede critical research, sharing, and innovation for the legitimate cybersecurity industry across all of the countries that implement the rule.

In the case of Italy, their implementation is essentially in name only with little to no enforcement mechanism in place. Take for example the Hacking Team, a Milan-based information technology company. The Hacking Team's public business model was to sell offensive intrusion and surveillance capabilities – the exact technology the Wassenaar Arrangement attempted to target with the new controls. However, the Italian export authorities granted a blanket global license to the Hacking Team allowing them to freely export their products around the world to many of the countries that the Wassenaar rule is trying to prevent from obtaining these tools.

Some companies who make products originally targeted to be controlled under the Wassenaar rule simply move to different jurisdictions to avoid onerous or explicit export controls on their products. The Gamma Group, owner of FinFisher (a type of surveillance software known as spyware) has opened subsidiaries and closed others in a number of EU countries and the British Virgin Islands, at least in part to what appears to avoid export controls. Indeed today, the legal status of the FinFisher product appears to be held by a completely separate entity from Gamma. Yet, they were still seen exhibiting their products at an arms fair in Paris recently.

The signatories to Wassenaar represent roughly 25 percent of the countries in the world. The group excludes many countries with growing cybersecurity industries and capabilities, such as Israel and China. Even if the rule were to be implemented uniformly, 75 percent of the world would not be bound by these regulations, putting those who rigorously implement and enforce the rule at a distinct competitive disadvantage. Moreover, the rule would not have its desired effect because the countries that have been accused of using malicious exploits for espionage or using surveillance software to spy on dissidents will still be able to obtain the controlled technologies from other markets. These technologies are already widespread and ubiquitous, and in many cases they are free on the Internet, so as to be nearly impossible to control.

During extensive international outreach and education regarding the impacts of the Wassenaar rule, some officials in European Union (EU) member nations have expressed a recognition that they may have overreached with the original Wassenaar control. Some have indicated a willingness to revisit the control and explore possible fixes at the upcoming Wassenaar Plenary. Indeed, many technical experts and EU export regulators have expressed concern that controls with no technical parameters or thresholds – such as the intrusion and surveillance software rules – will ultimately undermine the overall intent of the Wassenaar Arrangement if not addressed and corrected.

VI. Attempts to Re-write the Proposed U.S. Rule are Unworkable

As evidenced by the approximately 300 formal comments to the proposed rule, and as discussed in my testimony, a number of serious technical issues have been raised concerning these controls. To its credit, the DoC recognized the validity of these concerns and quickly withdrew the proposed rule in July. In the weeks and months since, industry and government have met multiple times seeking a common understanding of the issues with the rule, and possible ways to redraft it. The conversations that followed were extensive and frank – and ultimately unsuccessful. They failed for a simple, inescapable reason – the 2013 underlying Wassenaar controls are fundamentally flawed.

[8] Mimoso, Michael. "Citing Wassenaar, HP Pulls Out of Mobile Pwn2Own," ThreatPost, September 4, 2015. https://threatpost.com/citing-wassenaar-hp-pulls-out-of-mobile-pwn2own/114542/

There have been no suggestions for technical fixes to the language used in these controls because the issues with the rule are not technical. The core problem remains one of "intent"; fixes to technical definitions or product lists will not solve this issue. All multinational companies need to employ tools for computers or networks that have the functional specifications of the control parameters to avoid detection, defeat protective countermeasures, extract data or information, modify system or user data, and modify the standard execution part of a program or process to execute externally provided instructions. These are the exact hallmarks a malicious attacker's software would have and what an assessment team would hope to replicate. Thus, the issue becomes one of user intent.

Industry's concern, then, with the existence of such a rule is that it is not possible to use a technical description of the "malicious" tools used by malicious actors to distinguish them from the "legitimate" tools used by the cybersecurity industry – they are effectively the same tools – in an attempt to revise or carve-out exceptions that would allow legitimate cybersecurity uses. Therefore, the rule is both over-broad and will be ineffective in that it does not target that which the drafters presumably intended to target – those with malicious intent.

In addition, the use of exceptions by member states to enable a reasonable implementation of the controls leads to fatally flawed inconsistencies across the Wassenaar members. These inconsistencies lead to continuing questions by multinational companies regarding what is, and is not, controlled – creating a significant compliance burden. Moreover, the U.S. implementation creates a significant competitive disadvantage for U.S. companies who are held to a completely different standard than the rest of the member states.

It has proven to be very difficult, if not impossible to develop fair and consistent exceptions allowing unfettered transfers of such things as generic tools, not designed for purposes of "intrusion", which can also be used to generate, operate, deliver, or communicate with intrusion software. In order to hide from defenders, many new malware packages rely on existing features of complex operating systems to compromise devices and networks. While authorized teams use tools that would be controlled under Wassenaar, the malicious attackers would freely obtain the tools they need from non-commercial hacking sites. More advanced attackers and state-sponsored hackers would even develop their own custom tools – all while the legitimate users who need to develop the tools or use them for protection are limited from obtaining them while they wait weeks or months for their export licenses.

Altering the controls by developing carve-outs and exceptions are impossible to develop, enforce, and consistently apply. Limited exceptions other than defaulting to end use controls would render the controls ineffective. Realistically, the spread of these tools and technology cannot be limited when most if not all of the tools and technology are already available to non-member countries and large non-state criminal organizations. We believe creating carve-outs and exceptions will ultimately stifle innovation into new areas and techniques for cyber security defense, which cannot be predicted.

At the same time, any such list of exceptions would itself quickly become outdated as new cyber security products that do not match these descriptions are developed. And as noted above, any list of exceptions would be inconsistently applied across the Wassenaar states, thus creating uncertainty for multinational entities as to when a control applies and when it does not. Perhaps a better question to ask is whether the Wassenaar export control regime, or any export control regime, is the right approach to use in controlling the spread of malicious hacking tools and technology?

VII. Solutions Outside of the Wassenaar Arrangement Construct

As discussed throughout this testimony, Symantec believes that revising the proposed U.S. rule will not mitigate the negative effects of the original Wassenaar controls. However, there are more effective ways to address the problematic activity that the rule was designed to deter.

For example, the malicious cyber activity that is targeted under this rule could be countered under criminal law statutes that exist today. The U.S. government could dedicate additional resources to the FBI and federal prosecutors. Over the last decade the FBI and the Department of Justice have developed substantial experience in cyber investigations, forensics, and prosecutions. An export control regime managed by the DoC does not achieve these goals, especially since the technology will still be widely available throughout the world. Malicious cyber attacks are often based overseas, working with abusive foreign governments or underground criminal networks, which are threats that the DoC is neither resourced nor well-suited to address. Ultimately we go back to the fundamental flaw in the proposal – that technology-based export controls are the wrong mechanism to address cybercrime. Controls that are more capable of targeting the ill intent of the people using the software or technology are more suited for this purpose.

Sanctions are another tool that the U.S. government can use to address this threat. The Treasury Department's Office of Foreign Assets Control (OFAC) is already experienced and heavily engaged in this area. On April 1, 2015, the President issued Executive Order (EO) 13694 titled: *Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities.* Its purpose is to "enable the U.S. government to block the property and assets of extraterritorial actors involved in cyber attacks, who have otherwise been difficult to reach."[9] These cyber-enabled activities occurring outside the U.S. may constitute a significant threat to the "national security, foreign policy, or economic health or financial stability of the U.S." The Treasury Department's OFAC could dedicate more resources to carry out the EO and serve as a stronger global deterrent to malicious cyber actors. While OFAC just issued regulations implementing the EO last week, to date no designations have been issued.[10]

Conclusion

Since the U.S. cybersecurity export regulation was proposed in May of 2015, Symantec – together with a broader coalition of the cybersecurity industry and from across the critical infrastructure sectors – has engaged with the Administration about the significant negative consequences and dangers that this new export control regime will bring.[11] While many in the Administration have been receptive to our concerns, including the DoC and DHS, others have held steadfast to a position that ignores the realities of today's global cybersecurity ecosystem.

As described throughout my testimony, to implement the proposed U.S. regulation, or any variation of the underlying Wassenaar cyber rule, would have catastrophic effects on the cybersecurity industry, multinational corporations that rely on these technologies, and U.S. economic and national security. Any controls in this area should be focused on the intended use, rather than this widely-used technology upon which the world depends. The U.S. government should seek to utilize other authorities and mechanisms as described above to address this issue.

At a time when global cyber threats are increasing every day, it is imperative that the private sector and academia be able to conduct research and provide citizens, businesses, and governments with cutting-edge security products to keep pace with the growing threat. This is no time to restrict the availability of security tools and our ability to share information for cybersecurity purposes.

Symantec strongly recommends that the rule be remanded back to Wassenaar to be renegotiated and more narrowly defined. We look forward to continuing to work with the U.S. government and sharing our technical expertise to achieve an outcome that benefits cybersecurity in the U.S. and around the world.

---

[9] Perkins Coie, April, 2015. http://www.jdsupra.com/legalnews/president-issues-executive-order-to-bloc-76757/

[10] Steptoe & Johnson, LLP, January 7, 2016. "OFAC Issues Cyber-Related Sanctions Regulations." http://www.steptoe.com/publications-10990.html

[11] Coalition for Responsible Cybersecurity, http://www.responsiblecybersecurity.org

Mr. RATCLIFFE. Thank you, Ms. McGuire. The chair now recognizes Mr. Mulholland for his opening statement.

STATEMENT OF IAIN MULHOLLAND

Mr. MULHOLLAND. Chairmen Hurd and Ratcliffe, Ranking Members Kelly and Richmond, thank you for the opportunity to testify today at this important hearing. I'm Iain Mulholland, the head of the Engineering Trust and Assurance Group at VMware, and I am our senior security engineer. VMware is headquartered in Palo Alto, California, and is the fourth largest software company in the world, with 2014 revenues of over $6 billion and over 18,000 employees globally. Ironically, I may be one of the few people in the room, other than, perhaps, Ms. Ganzer, who has actually spent any time in Wassenaar, as my then-fiancee lived there in the 1990s. I spent a summer in Wassenaar reading books on computer security during my transition out of service in the British military.

I now have almost 20 years' experience in the software security engineering field. I came to the U.S. in 2002 as one of the early members of the Microsoft Trustworthy Computing Group. And in 2011, I established VMware's Product Security Group.

If implemented, the 2013 Wassenaar Arrangement could undermine our strong security posture and hinder our ability to adequately protect our customers and our products. It would introduce significant hurdles to rapidly receiving and sharing threat information, in particular, vulnerability exploit code that is critical to the swift development of security patches that protect software users, something that Chairman Hurd alluded to.

This introduction of a requirement to apply for and obtain licenses during critical, time-sensitive responses to security vulnerabilities, which may already be under active exploitation, creates an asymmetry that is to an attackers' advantage, since, unlike the defender, the attacker has few such constraints.

In my written testimony, I included three different examples that speak to the core challenges that implementing the 2013 rules would present not only VMware, but as some testimony has already alluded to, other U.S. technology companies. In the interest of time, I would like to share one of them with you. In the last 12 months, VMware has collaborated with several small security research organizations in Europe to remediate critical security vulnerabilities that they identified in our products. These vulnerabilities, if left unpatched, could have allowed a malicious attacker to take complete control over critical infrastructure. During the course of our investigations, researchers often provide VMware with sample exploit code that demonstrates the flaw to our security response team.

Exploit code is often key in accelerating the speed with which our engineers are able to understand the flaw and develop a patch to protect our customers. If a picture paints 1,000 words, then in the field of software security, the exploit is our picture. In one example, the security researcher was in Poland, his parent company, in the Netherlands, the coordinating VMware incident response team in the U.S. and Canada, and the team responsible for developing the security patch, in India. In addition, several of our U.S.-based em-

ployees were non-U.S. persons. In this example, VMware and the researcher would have required multiple licenses, one from Poland to the Netherlands, from Poland to the U.S., from the Netherlands to the U.S., from the U.S. to Canada, and several within the U.S. just to share information across cubical walls with non-U.S. persons based in the United States.

Security vulnerability reports typically come through our industry standard security at VMware.com email address, using a security research protocol that has been in use in our industry for over 15 years. In 2015 alone, over half the security vulnerabilities reported to VMware came from individuals or organizations located in Wassenaar countries. In most cases, an export license would have been required for the researcher to report the security issue to us. A security researcher may not even have known who or where they were exporting an export to, since security at VMware.com is staffed on a rotational basis by a global team, half of whom are outside of the U.S. or non-U.S. persons.

It is improbable that these small research companies or individuals will take on the administrative and financial burden of applying for potentially multiple export licenses simply to report a security vulnerability. And as a result, this important source of information will dry up, or much worse, end up in the underground vulnerability market, leaving vulnerabilities unreported, unpatched, and under active exploitation.

Moving forward, we recommend the BIS and the Department of Commerce continue to keep all options on the table. We applaud them for reconsidering their original draft, and hosting a series of public forums with a range of stakeholders to try and find a reasonable solution which we are pleased to participate in.

Ultimately, however, the U.S. should return to Wassenaar and renegotiate the 2013 arrangement. We live in a global digital ecosystem that is not constrained by borders. We receive information about threats that affect the security of our products and our customers from all over the world. Even if the U.S. fixes its domestic policy, it will not enable us to continue to receive and share critical and timely information that affects the security of our customers on products from outside our borders. We must have the tools and resources on hand to act immediately and continue to provide world class secure software and services and ensure customer safety. Unfortunately, the 2013 Wassenaar agreement would undermine our ability to do so.

I applaud the leadership of the committee for holding this hearing today. Thank you for the opportunity to testify. And I look forward to answering your questions.

[Prepared statement of Mr. Mulholland follows:]

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, Ranking Member Richmond and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Iain Mulholland, head of the Engineering Trust & Assurance Group for VMware. I have nearly 20 years' experience in the product security field, including establishing VMware's Product Security Group in 2011. Before VMware, I worked for a number of leading technology companies, including in 2002, when I was a founding member of the Microsoft Trustworthy Computing Group.

My employer, VMware, is the fourth largest software company in the world, with 2014 revenues of over $6 billion and over 18,000 employees. VMware has more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. VMware serves all sectors of the U.S. Government; including the Department of Defense, the Civilian agencies, and the Intelligence Community, as well as state and local governments. The company is headquartered in Silicon Valley with 140 offices throughout the world.

VMware is a leading provider of software-defined solutions that make data centers across the globe operate more efficiently and securely and that enable both government and commercial organizations to respond to dynamic business needs in on-premise datacenters, in the cloud, and on personal computers and mobile devices. VMware is providing enhanced security to commercial and government customers globally through its pioneering role in redefining how we build and secure networks, data centers, computers and devices.

Concerns with the 2013 Wassenaar Arrangement

The Wassenaar Arrangement was originally established in order to contribute to regional and international security, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies. There are 41 nations, including the U.S., who are part of the Wassenaar Plenary. In order to implement policies from the Wassenaar Arrangement, each participating country has the ability to implement the policies through the application of its national legislation and policies. There is no harmonized implementation across the 41 nations.

On May 21, 2015, the Department of Commerce's inter-agency "Bureau of Industry and Security (BIS)" released a draft proposal to implement the 2013 Wassenaar Arrangement. As put forth in the Wassenaar Arrangement, the draft BIS proposal would, in our view, implement much stricter export controls on security technology, including "intrusion software."

The security and protection of our customers is an extremely high priority for VMware and we have made significant investments to proactively ensure the security of our products, services and infrastructure. The 2013 Wassenaar rules would severely impact VMware's ability to test and share code used to test for security vulnerabilities in our products, services and global infrastructure. This would lead to less secure products and in turn, less secure customers. VMware, like many other global U.S. companies, exchanges security-related information across borders as part of its daily operations to conduct research and development, security testing, or address any network breaches

instantaneously, whether it be within our own internal networks, or the networks of our technology partners, business customers, or governments.

Like others in the technology space, we share the concerns about the challenges to be required to apply for and obtain a great number of export licenses to cover the vast range of information-sharing and other security-related activities. This could create a massive backlog and be extremely time-consuming, creating a situation for companies, like VMware, to not be able to share threat information instantaneously and in real-time to prevent or stop a cyber attack on our network, or against the infrastructures of our technology partners, business customers or government. This would only give malicious hackers a window of opportunity to exploit vulnerabilities, knowing that companies like ours would have our hands tied for an extended period of time while applying for and awaiting export licenses to be approved.

The global digital ecosystem is experiencing a level of cyber attacks and sophistication that we have never seen. In order to secure and adequately protect our customers, products, services and networks against these highly sophisticated entities we must utilize every security tool we have in the toolbox.

Examples of how Wassenaar Rules Could Undermine Cyber Posture

I would like to share for the record some of my personal experiences that I believe speak to the core challenges that implementing the current Wassenaar rules would present not only for VMware as a company, but other similar U.S. companies.

1) In the last 12 months, VMware has collaborated with several small security research organizations in Europe to remediate critical security vulnerabilities they had identified in our products. These vulnerabilities, if left unpatched, could have allowed a malicious attacker to take complete control of critical infrastructure. During the course of the investigation of these issues, the researchers have typically provided VMware with sample exploit code that demonstrated the flaw to VMware's Security Response team. Exploit code is often key in accelerating the speed with which VMware's engineers are able to understand the flaw and develop a patch to protect customers.

In one example the security researcher was in Poland, his parent company was in the Netherlands, the coordinating VMware Incident Response Managers in the US and Canada, and the team responsible for developing the security patch in India. In addition, several of the US-based VMware Security Engineers were non-US persons. In this example, VMware and the Security Researcher would have required multiple export licenses – one from Poland to the Netherlands, one from Poland to the US, one from the Netherlands to the US, one from US to India and several from the US to share information with US-based VMware employees who are not non-US Persons. It is highly unlikely that a researcher based in Poland working for a company based in the Netherlands would have the means or inclination to get multiple export licenses in this scenario and even if they did, this would have introduced delays of many days if not weeks. Furthermore, it is impractical that the individuals charged with leading VMware's response to reports of security vulnerabilities in our products would not be

able to view said reports without first obtaining an export license, nor would they be able to share this information with key team members unless covered by an appropriate export license. In all likelihood, under the proposed Wassenaar rules this flaw would have gone unreported and customers would continue to be vulnerable to this critical security flaw.

In 2015 alone, over half of the security vulnerabilities reported to the VMware Security Response Center from external parties have come from individuals or organizations located in Wassenaar countries. In most cases, an export license would have been required for the party to report the security issue to VMware. A security researcher would likely not even know where they were exporting to since VMware employs security engineers of multiple nationalities in multiple time zones to provide ongoing monitoring for reports of security vulnerabilities in our products. It is highly improbable that these small research companies or individuals will take on the administrative and financial burden of applying for export licenses simply to report security vulnerabilities and as a result, this important source of information will dry up, leaving vulnerabilities unreported and customers less secure.

2) VMware has made a significant investment in the security of our products and we have an established Product Security team that executes a Secure Development Lifecycle (SDL) during the development of our key products. This SDL program is one of the most mature product security programs in the software industry. During the normal course of this SDL, VMware engineers will often develop exploit code to demonstrate security vulnerabilities in our products and services. These exploits are used to test product security, demonstrate that products have been effectively patched, and act as training aids when conducting security training for our global engineering community. These exploits are developed and shared in the course of our daily research and development with engineers across the globe, often with engineers in several different countries and of different nationalities collaborating in real time. As such the ability to develop and rapidly share exploit code within our own engineering community without hindrance is critical to helping ensure the security of VMware products and services.

3) VMware is an active member of a number of software industry product security initiatives including the Software Assurance Forum for Excellence in Code (SAFECode), The Industry Consortium for Advancement of Security on the Internet (ICASI), and the Linux Foundation's Core Infrastructure Initiative. VMware regularly shares security information with participants of these and other forums. Indeed, security is often seen as a leveler and we often share threat information with competitors in an effort to ensure that our mutual ecosystems are protected. For example, in 2014 several significant security vulnerabilities affected major cryptographic implementations. VMware identified that a very commonly used community test for one such vulnerability was inaccurate in how it reported the vulnerable state of certain servers, including a number of VMware server products. The test incorrectly reported that servers were secure when in fact they were not, leading customers into a dangerous false sense of security. Within a matter of hours of the vulnerability becoming known to the community, VMware security engineers released a corrected version of the test, which was in effect a benign exploit, as the vulnerability condition could not be accurately tested at scale in any other

manner. The security community quickly incorporated this corrected test into their frameworks so that customers could correctly assess the security of their infrastructures.

Had we been required to seek an export license in this example, we would have faced a situation where a substantial number of customers initially believed they were secure when they were not, until we were able to release new tests that had the correct export licenses. This situation could have taken many days to resolve instead of being fixed within hours.

With that said, you can see clearly that the 2013 Wassenaar rules, if implemented, will have the exact opposite effect of its intended purpose, meaning it could leave consumers, businesses, and governments less safe from cyber attacks, not more.

Next Steps

Since BIS released its original draft proposal in May, the Department of Commerce and BIS held a series of public forums with stakeholders, ranging from government officials to industry representatives and academics. VMware was pleased to participate in the stakeholder process to work constructively with BIS, the Administration and other stakeholders to find a solution moving forward. BIS should be applauded for their efforts for being transparent with its public forums and working with all stakeholders to better understand the consequences of implementing the 2013 Wassenaar Arrangement.

I would also like to applaud the congressional attention to this issue. In addition to this important congressional hearing, the bipartisan congressional letter spearheaded by Chairman Michael McCaul, Congressman Jim Langevin and signed by over 120 Members of Congress demonstrated the importance for the U.S. to re-think its strategy relating to the 2013 Wassenaar Arrangement.

Moving forward, we recommend that BIS and the Department of Commerce continue to keep all options on the table. This includes two options. The first, we strongly support BIS amending its original draft to reflect some of the concerns raised at its public forum. However, we believe, that even if the U.S. gets its policy right, it still will not be sufficient given the increasing global cybersecurity threats we are facing. That is why, in my opinion, the more effective option is for the U.S. to return to Wassenaar and renegotiate the original 2013 Wassenaar Arrangement dealing with export security controls.

The reality is that VMware, like other global technology companies, not only receives ever-dynamic cyber threat information from inside the U.S., but we also receive a large number from oversees as well. The fact is, with data moving across borders instantly, the cybersecurity ecosystem is not confined to borders. In order to continue to provide world-class secure enterprise software and services and ensure customer safety, we must be able to act on a moment's notice whether that information is coming from the U.S. or abroad. We must have the tools and resources on hand to act immediately.

Summary

We strongly believe that if the 2013 Wassenaar Arrangement is implemented it could undermine our security posture and hinder our ability to adequately protect our customers, products, services and networks. The cyber threats are rapidly changing and are extremely sophisticated. We, collectively as an industry, are charged with providing the world's digital security. To be effective, we will need every tool at our disposal to prevent or mitigate cyber attacks on not only our customers' networks, but our own. The 2013 Wassenaar Arrangement would take away critical tools to counter cyber attacks. It would hinder our ability to prevent or mitigate cyber attacks not only on our customers' networks, but on our own.

We applaud BIS and the Commerce Department for reconsidering its original draft proposal, and hosting a series of public forums with a range of stakeholders to try to find a reasonable solution. Ultimately, however, the U.S. should return to Wassenaar and renegotiate the 2013 Wassenaar Arrangement. We live in a global digital ecosystem. We receive cyber threats against our networks and our customers from all over the world. Even if the U.S. fixes its policy here domestically, it will not enable us to continue to receive critical and timely threat information-sharing from outside our borders.

VMware appreciates the opportunity to share our thoughts on this very important issue. We applaud the leadership and vision of the Chairmen and Ranking Members for holding this hearing. VMware looks forward to continuing to participate in efforts to find solutions to help resolve this issue. Thank you again for the opportunity.

Mr. RATCLIFFE. Thank you, Mr. Mulholland. Ms. Goodwin, you're recognized for 5 minutes.

STATEMENT OF CRISTIN FLYNN GOODWIN

Ms. GOODWIN. Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, Chairman McCaul, Chairman Thompson, members of the subcommittees, my name is Cristin Flynn Goodwin. And I'm assistant general counsel for Cybersecurity at Microsoft. I advise a wide range of teams on cybersecurity legal issues, and I manage Microsoft's government Security Program working with governments around the world. Thank you for convening today's hearing and your bipartisan leadership to support our Nation's cybersecurity. Microsoft has a deep commitment to cybersecurity. And I'm happy to be here today to discuss our perspective of the Wassenaar Arrangement's controls on intrusion software agreed to at the December 2013 Plenary and the proposed U.S. implementation.

As detailed in my written testimony, Microsoft believes the Wassenaar Arrangement's approach to controlling intrusion software and the broad export licensing requirements proposed in the U.S. would undermine security research, incident response, cyber collaboration, and product innovation. We agree with your assessment, assessed in a bipartisan letter to Ambassador Rice last month, that without a significant overhaul, these broad licensing requirements could seriously hinder national security.

The intent of the drafters of these provisions was to prevent the export of surveillance software to criminal organizations or repressive regimes, which is admirable and important. Unfortunately, due to the very broad definition of intrusion software, extensive range of security technologies will now be subject to broad and burdensome licensing requirements in the U.S. If left unchanged, the proposed definition will have a chilling effect on the development of products and services and on the discovery of existing vulnerabilities. It will also significantly impact security incident response, and create new barriers for those seeking to secure themselves against increasingly persistent and sophisticated cyber threats. To demonstrate the impact, consider these three very common cybersecurity scenarios.

First, a large critical infrastructure provider based in Germany is concerned that there is an attacker present on its corporate network and stealing sensitive information. The company calls in an American security company to come to Germany to help investigate whether the attacker is still present, and to use tools to find out what the attacker might be trying to steal or access without tipping them off.

Second, a cybersecurity researcher with a small company in the United States finds a new piece of malware that hides itself on a user's machine, and then automatically deletes log files that indicate where an attacker is hiding on a machine. The researcher wants to share his analysis of the malware and collaborate with a software vendor in the U.S.

Third, an American software company is developing a new product for commercial sale. Its internal security team, with members

in the U.S., Australia, and Japan, wants to develop a tool that will help them test the product's security measures before it is sold.

What do these scenarios have in common? Security response, collaboration, and product innovation stops until new export licenses can be processed, which can take weeks or even months. It also means that the attacker will be present for weeks on the German network. The malware identified by the researcher will continue affecting machines. And the software company will be delayed in its effort to develop a new product.

Clearly, none of this is in the best interest of American cybersecurity. The United States must lead the effort to re-set this flawed approach internationally. Security experts should not have to pick up the phone in the middle of the night to call in an export control adviser to determine whether they can share certain technical information about an ongoing attack or as part of their day-to-day work, wait to collaborate with internal or external colleagues on security priorities. In today's global security environment, the ability to collaborate with peers and colleagues should be the default, not the exception.

As both of your subcommittees know well, developing cybersecurity policy requires a deep understanding of the problem, broad input from experts, engagement with the executive branch and Congress, and a transparent process.

Regrettably, to the detriment of cybersecurity, the Wassenaar Arrangement definition of intrusion software does not reflect this type of inclusive process. It must be renegotiated.

In conclusion, Microsoft is a committed participant in the public-private partnership, and strongly encourages Congress and the executive branch to take the necessary steps internationally, and with our Wassenaar partners, to undo the overly broad and complicated export control requirements. Concurrently, the administration should suspend any related rulemaking efforts until a new agreement can be reached, making use of a robust, consultative process.

Ms. GOODWIN. I commend you for examining this issue today, and thank you for the opportunity to testify. I look forward to answering your questions and working with you on this important issue. Thank you.

[Prepared statement of Ms. Goodwin follows:]

Written Testimony of Cristin Flynn Goodwin
Assistant General Counsel for Cybersecurity at Microsoft Corporation

Oversight and Government Reform Subcommittee on Information Technology
Homeland Security Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies

Joint Subcommittee Hearing on Wassenaar: Cybersecurity & Export Control
January 12, 2016

Introduction

Chairman Ratcliffe, Chairman Hurd, Ranking Member Richmond, Ranking Member Kelly, and members of the Subcommittees, my name is Cristin Flynn Goodwin, and I am Assistant General Counsel for Cybersecurity at Microsoft Corporation. I advise a wide-range of teams inside Microsoft on cybersecurity legal issues globally and I oversee Microsoft's Government Security Program, where we work with governments around the world on security.

Microsoft is a global company operating in over 120 countries, with services and products that consumers, enterprises, and governments use on a daily basis. Eighty percent of the Fortune 500 and millions of consumers rely on our cloud services.[1] This growth and scale in our cloud business helps us appreciate the complexity of meeting security challenges and protecting customers around the world. It is Microsoft's commitment to security that brings me here today to discuss our assessment of the challenges in implementing the Wassenaar Arrangement's controls agreed to at the December 2013 Plenary on intrusion software and related items.[2]

As the Subcommittees know well from the recent success on the Cybersecurity Act of 2015, legislating cybersecurity requires a deep understanding of the problem space, broad input from experts and the private sector to ensure thoughtful technical impact and applicability, support from major stakeholders in the Executive Branch, and the open and well-known legislative process to move the issue forward. In the case of the intrusion software definition coming out of the Wassenaar Arrangement, and its proposed implementation from the Department of Commerce, this issue does not reflect the same sort of consensus.

The proposed definition, if left unchanged and implemented, applies "almost universally to the building blocks of security research" and will have a "chilling effects on the development of anti-surveillance

---

[1] "Satya Nadella and Scott Guthrie: Microsoft Cloud Briefing," Microsoft News Center, October 20, 2014, available at: http://news.microsoft.com/speeches/satya-nadella-and-scott-guthrie-microsoft-cloud-briefing/.

[2] The Wassenaar Arrangement is a 41-nation regime designed to advance "regional and international security and stability by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies." Its members include a majority of European nations, as well as Canada, Russia, Japan, and Australia. The Agreement aims to prevent destabilizing accumulations of certain capabilities and to prevent the acquisition of these items by terrorists.[2] Wassenaar is a consensus-based organization; once consensus is reached, the Member States implement the agreements domestically in accordance with local legislation. Quote and information available at www.wassenaar.org.

measures and on the discovery of existing vulnerabilities."[3] We have the opportunity to re-set the international approach and its domestic implementation, and ensure that security responders and technology innovators around the world can respond to threats and vulnerabilities in real-time, as they do every day. At a time when we are all looking to empower security defenders and provide them with the tools and capabilities they need, we cannot take a significant step backwards.

Microsoft strongly encourages Congress and the US Government to re-engage Wassenaar Arrangement member states, undo the overly broad, overly complicated export control requirements, and suspend any related rulemaking efforts until a new agreement can be reached.[4] As a committed participant in the public private partnership in the United States, we are eager to engage on cybersecurity regulation and to provide any technical expertise and perspective needed going forward.

We commend both subcommittees for examining the use of export control regimes to regulate cybersecurity, and we welcome the opportunity to contribute to this important dialogue.

My testimony will focus on four areas:

1. The Wassenaar definition of intrusion software and the problems that arise from the overbroad definition and controls;
2. The impact of the proposed regulatory approach on innovation and security response;
3. The importance of the public private partnership in cybersecurity regulation; and
4. The role of governments in establishing cybersecurity norms that curtail the uses of surveillance technologies.

1. Why Words Matter: Defining the Problem and "Intrusion Software"

a. Defining the Problem

Microsoft is a staunch supporter of the principle that technology should not be used to violate human rights, or to harm or impede those that seek to advance the cause of human rights. In that vein, the original intent of the Wassenaar Arrangement drafters is admirable and important. Unfortunately, due to the overbroad definition of intrusion software, the broad scope of items subject to control, and the burdensome licensing requirements proposed in the United States, this Proposed Rule would create a set of regulations that constrain security and innovation and may diminish the capabilities of enterprises and people to secure themselves against increasingly persistent and sophisticated cyber threats.

Although many Wassenaar proceedings are confidential, Microsoft understands that the original intent behind these controls was to restrict the export of sophisticated surveillance systems to authoritarian governments. Such systems, like those developed and sold by companies like Gamma Group (owner of FinFisher) and Hacking Team are reportedly used to spy on or otherwise repress political dissidents and

[3] "Why Wassenaar's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk – And How To Fix It", Sergey Bratus, et al., October 9, 2014, available at: http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

[4] For additional detail on the challenges with the Proposed Rule, please consult Microsoft's "Comments on Wassenaar Arrangement Plenary 2013: Intrusion and Surveillance Items" available at: http://mscorp.blob.core.windows.net/mscorpmedia/2015/07/Microsoft-Intrusion-Software-Submisson-BIS-2015-2011-RIN-0694-AG49.. .pdf.

other citizens.[5] These sophisticated turnkey systems are claimed to permit the targeting and monitoring of an individual's phone calls, emails, and other communications.

Limiting the sale of sophisticated surveillance technologies to governments or other entities that could abuse the technology and violate laws or rights of others is a very real and very important challenge that needs to be addressed. Appropriately tailored export control regulations may be one part of an overall approach to controlling transfers of these technologies. However, in order to address concerns about abuses of surveillance software, or other similar topics in the future, it is important that the involved governments clearly articulate the challenge and engage technical experts from the private sector well before future Wassenaar votes take place. Given the broad dissent and need for clarity on the problem scope, applying principles from the cybersecurity norms discussion and driving for broader nation state and industry consensus prior to international agreement and regulation is a better approach. Due to the fact that the intrusion software issue has already gone through Wassenaar voting, it may be more realistic to encourage Wassenaar members to apply the principles of the cybersecurity norms debate to its work and reset this discussion from the beginning.

b. Defining Controls Related to Intrusion Software

The Wassenaar members in 2013 used a very challenging approach to try to define what it sought to control. First, as has been commented on by many stakeholders, the Wassenaar Arrangement agreed to a very broad definition of "intrusion software":

> *Software specially designed or modified [i] to avoid detection by monitoring tools, or [ii] to defeat protective countermeasures, of a computer or network-capable device [including mobile devices and smart meters], and [iii] performing any of the following:*
>
> *(a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data; or*
>
> (b) *The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions.*

To those who are not technical information technology (IT) experts that definition might appear quite narrow. However, it "covers common and essential software techniques used throughout software engineering, not just potentially nefarious ones unique to malware and attack tools. In fact, these techniques are used by computer security products, remote management software, antivirus, enterprise

[5] *See, e.g.*, Bill Marczak, Written Evidence to the UK Parliament, *Export of British-Made Spyware Targeting Bahraini Activists*, November 19, 2012, available at: http://www.publications.parliament.uk/pa/cm201314/cmselect/cmfaff/88/88vw43.htm; *see also* Response of the UK Secretary of State for Business Innovation and Skills, *Export Controls for Surveillance Equipment - Proposed JR*, August 8, 2012, available at: https://web.archive.org/web/20140816043658/https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/2012_08_08_response_from_tsol.pdf.

reliability and monitoring, and operating systems."[6] Then, in an added layer of complexity, the Wassenaar controls and licensing obligations are applied to the following items *related* to such intrusion software (among other items):

(a) Systems, equipment, components and software specially designed or modified for the generation, operation or delivery of, or communication with intrusion software; and

(b) Technology (*i.e.*, technical data and technical assistance) for the development of intrusion software, or for the development, production or use of equipment or software specified in (a) above.

Because the Wassenaar Arrangement text is not self-executing, each member state then in turn implements the agreed-upon controls domestically. The United States implementation was proposed by the Department of Commerce (Commerce) Bureau of Industry and Security (BIS), in a Federal Register notice in May 2015 ("Proposed Rule") that took some in the security community by surprise.[7]

Security teams around the world looked at the overbroad definition, exacerbated by the BIS proposal on implementation, and the reaction from the security community was quite vocal, questioning how it would be possible to continue developing new products and services, or to fight attacks and threats, if the proposed regime became the law in the United States. Microsoft engineers expressed concern that, if implemented, triaging vulnerabilities with security researchers in the Microsoft Security Response Center[8], assessing malware in the Microsoft Malware Protection Center[9] or developing tools with internal teams could become a burdensome and time-consuming exercise of government filings, documentations, and forms, and not innovation.

This reality is already affecting the security community. One security conference was cancelled in Japan, citing "'the complexity of obtaining real-time import/export licenses in countries that participate in the Wassenaar Arrangement. . . .'"[10] The prospect of untangling a web of export filings for a cadre of

---

[6] "Why Wassenaar's Definitions of Intrusion Software and Controlled Items Put Security Research and Defense at Risk – And How To Fix It", Sergey Bratus, et al., October 9, 2014, available at: http://www.cs.dartmouth.edu/~sergey/drafts/wassenaar-public-comment.pdf.

[7] "Head Scratching Begins on Proposed Wassenaar Export Control Rules," Michael Mimoso, Threat Post, May 21, 2015, available at: https://threatpost.com/head-scratching-begins-on-proposed-wassenaar-export-control-rules/112959/. *See also*, "Experts Concerned About Effects of Proposed Wassenaar Cybersecurity Rules," Eduard Kovacs, Security Week, May 26, 2015, available at: http://www.securityweek.com/experts-concerned-about-effects-proposed-wassenaar-cybersecurity-rules.

[8] More information about the Microsoft Security Response Center available at: https://technet.microsoft.com/en-us/library/dn440717.aspx.

[9] More information about the Microsoft Malware Protection Center available at: http://www.microsoft.com/security/portal/mmpc/default.aspx.

[10] "Pwn2Own Tokyo hacking contest trashed, export rules blamed" Richard Chirgwin, The Register, September 3, 2015, available at: http://www.theregister.co.uk/2015/09/03/pwn2own_tokyo_trashed_wassenaar_blamed (quoting official from the event's sponsor).

international security researchers working in real-time to create security solutions to challenging problems simply stifled the research altogether. Even before implementation, the overbroad definition and scope of the controls are already having an impact on the security community's ability to collaborate and respond.

2. Impact of the Current Approach on Innovation and Cybersecurity

a. How Microsoft is Impacted by the Current Wassenaar Approach

Microsoft has devoted significant resources and personnel to extensive, critical, and time-sensitive research and development and other defensive security activities to protect our software, our services, and our networks against cyber and other security vulnerabilities. This work is essential not only to protect Microsoft's own networks and services, but more broadly to protect the networks and data of Microsoft's customers and users, including US Government users, such as the Congress of the United States. These activities, which are vital to protecting our nation's IT infrastructure, would be severely impeded by the Proposed Rule if implemented as drafted.

Given the global nature of product development and *defensive* security activities and the involvement of nationals from dozens of countries — including employees of Microsoft and its large number of third party security partners — Microsoft estimates that current activities would require the issuance by BIS of hundreds or thousands of export licenses. Millions of Microsoft customers, including the US Government, would likely face increased software and other security vulnerabilities that could be exploited by state and non-state actors, and our customers, as well as the security community, would feel the impact of slower incident response, and delayed product updates and services as security is put on hold due to licensing obligations.

Internally, Microsoft has a diverse community of teams involved in security. Some of these teams are well known, like the Microsoft Security Response Center, the Microsoft Malware Protection Center, or the Digital Crimes Unit[11]. Others are more internally focused, and concentrate on product development (such as Windows or Office and our cloud services). Microsoft Consulting Services also supports client security needs around the world, including the US Government and government contractors. Each of these teams includes significant numbers of non-US citizens.

Here is an example of a type of event that happens over 1,000 times a year at Microsoft. The Microsoft Security Response Center (MSRC) receives an unsubstantiated tip from a researcher in Switzerland, which claims to contain a proof of concept of a vulnerability, some reproduction code, and a tool that the person used to get the vulnerability to reproduce. The MSRC employee, a US national, needs to discuss the technical details of the proof of concept in order to validate the vulnerability, but to reach back to the researcher in Switzerland, he would likely need a license (or at least spend time determining whether a license is needed). Instead, he reaches out to another employee on his team to help. She is a citizen of Poland working in the UK. If not already authorized, our US national needs to contact Microsoft's Global Trade team which will help the employee prepare a filing to obtain a license to do that validation. The license application will take 6 – 10 hours to prepare, and then approximately 30 days to be approved. Once approved, and the technical exchanges occur, the MSRC validator writes some code that helps her test the vulnerability and test a potential idea for mitigation, along with an

[11] More information on Microsoft's Digital Crimes Unit available at: http://news.microsoft.com/presskits/dcu/.

accompanying technical explanation. However, before these materials can be shared with the development organization, including developers of many nationalities, additional licenses may be needed to share the information with the developers, depending on their nationalities. This is simply an unworkable process just to start an investigation for certain vulnerabilities.

b. Specific Examples of Impact Arising out of the Intrusion Software Definition

The private sector has voiced significant concerns over the overbroad intrusion software definition as well as the related technology and software controls. Microsoft has identified nine different areas of major impact in the security space should these controls remain in place, and the implementation adopted. Each of these areas is detailed below, and ranges from present and immediate concerns (as in the ability to deploy penetration testing tools) to more forward-looking concerns (such as machine to machine sharing creating an export or re-export licensing obligation). In all of these areas, Microsoft's security teams are not simply passive recipients of information or tools; to be effective and timely, the teams must be engaged in active creation, response and sharing of software and technology that is likely to be controlled under the Proposed Rule.

Issue	Description	Used For
Penetration Testing	Software created or used to evaluate and improve the security of services and software that Microsoft develops and operates. Includes proprietary software and open-source software that Microsoft has specially designed or modified for particular purposes.	Used to monitor internal systems, ensure compliance with security policies, and help protect systems. Microsoft also reverse engineers pen testing tools used by bad actors in order to protect customers.
Malware Research	Malware, exploit code, and reported vulnerabilities, including malware that meets the definition of intrusion software.	Microsoft performs extensive analysis on malware, including reverse engineering the code to identify how it was put together. Microsoft also creates *new* code, including new intrusion software, to illustrate the risks of the particular malware or malware family
Vulnerability Testing	Similar to penetration testing, Microsoft uses both proprietary tools and open source tools that are specially designed or modified in response to specific intrusion software-related attacks.	Mitigating impacts of vulnerabilities, identifying new vulnerabilities, and enabling software engineers to reproduce and test software patches, updates, and upgrades.
Security Tools	This is a broader class of tools used in security, including debuggers, file	Identifying vulnerabilities, modifying software to enhance operability or decreasing security risks

	fuzzers, and other automation used to support security.	
Application Compatibility, Interoperability and Work-Arounds	Microsoft develops and deploys "shims" which are technology "work-arounds" to aid in the compatibility of software programs with its operating systems.	Shims or work-arounds modify the intended function or path of a file in order to enable compatibility with other devices or interoperability with other software.
Information Sharing	Receiving and sharing thousands of threat reports, vulnerability issues, and other security related issues on Microsoft products and services and third party products and services in the Microsoft ecosystem. Collaborating on planned and ad hoc issues that arise on security.	Incident response, mitigating vulnerabilities, investigating new issues, sharing information to help raise security awareness amongst others, and generally protecting the computing ecosystem.
Supporting Customers	Microsoft Consulting Services provides technical and other services on-site with customers around the world leveraging Microsoft tools and technologies.	Used to investigate breach responses, conduct penetration tests, review software and security issues, and create recommendations on improving security.
Engaging the Security Community	Working directly with security researchers, third-party companies, hosting competitions, participating in conferences, and engaging on difficult security issues to improve product and services security.	Includes sharing information, technology, tools, ideas, and collaboration; can include hosting "bug bashes" or awarding prizes,[12] paying for "bug bounties," publishing research,[13] attending conferences, and creating new tools, technologies, and tactics to improve security.
Automated Exports and Re-Exports	Automation is the future state of security and is continuing to change the security landscape. Machine to machine information sharing allows automation and machine learning to make adjustments without human interaction, although the	Microsoft engages in a growing use of automated software programs and custom developed tools, which can include software that automatically exports and re-exports items; the Proposed Rule

[12] See, e.g., Microsoft's Blue Hat Prize: http://www.microsoft.com/security/bluehatprize/.

[13] "UK Student's Research a Wassenaar Casualty," Michael Mimoso, threatpost.com, July 6, 2015, available at: https://threatpost.com/uk-students-research-a-wassenaar-casualty/113625/ (highlighting a restricted portion of the student's dissertation on expanding bypasses for Microsoft's Enhanced Mitigation Experience Toolkit).

	information can move between US and non-US servers.	does not yet contemplate machine to machine exports and re-exports.

c. The Impact of the Licensing Burden on Industry and BIS

The Wassenaar Arrangement specifies *what* is to be controlled, but does not identify specific levels or methods of control that each member state should apply. The US licensing requirements that would be imposed under the Proposed Rule compound the serious problems created by the overbroad Wassenaar definition of what is controlled. While other Wassenaar members appear to apply a permissive licensing regime, the United States proposes to require specific prior export licensing for virtually any export or re-export - including disclosures to foreign nationals in the United States - of any controlled item to any destination other than Canada.

Microsoft estimates that the Proposed Rule would require hundreds or thousands of licenses for the export, re-export, and/or deemed export of items. Microsoft has an experienced and well-developed export control compliance program; however, no compliance team could prepare this many license applications, to say nothing of managing compliance with the terms and conditions of issued licenses. The burden on development and security teams to assist in the creation and completion of and compliance with these licenses would clearly impact product and service creation, customer support, and security. Today, an average license submission with readily available contacts and information needed takes between 6 to 10 hours to prepare. For more complex licenses or issues that require more technical investigation, that range can increase significantly.

It is a reasonable presumption that BIS will lack the capacity to review and issue the volume of licenses for all of the companies, universities, individual researchers, and other organizations that will require such licensing. Today, we expect an average of 30 days to receive an approval on a license application, with more complex issues taking 90 days or longer. Waiting periods will likely increase as the volume of licenses increases exponentially.

Moreover, the involvement of foreign nationals (either employed by Microsoft or a third party) occurs in every facet of security today. Response occurs 24x7, using "follow the sun" capabilities, whereby security issues are transferred to teams in different time zones so that security work can progress around the clock. This real-time activity cannot be postponed for days, let alone weeks or months, while Microsoft prepares a license application and BIS processes it, including referral to the Defense Technology Security Administration. Export licenses also could not be obtained in advance for every situation for which export authorization may be needed, since the specific controlled technology or software to be exported or re-exported, the identity of the foreign nationals or entities receiving it, and destinations with whom the items will be shared, generally will not be known in advance.

Finally, as part of some of the activities described above (to investigate or mitigate threats), in some instances Microsoft exports and re-exports items that have or support rootkit and/or zero-day exploit capabilities. According to the preamble to the Proposed Rule, a policy of presumptive denial would apply to license applications for such items, and therefore exports and re-exports that are a core aspect of critical security activities apparently would be prohibited from occurring, putting customers at risk.

d. Impact on Congressional Priorities

The US Congress recently passed information sharing legislation that would facilitate the sharing of cyber threat information within the private sector, as well as between the private sector and the government. The proposed regulation has interesting ramifications for the Cybersecurity Act of 2015 as well. As the Subcommittees are well aware, widespread sharing of information about threats, vulnerabilities, and adversary capabilities and techniques is critical to ensuring security and privacy. Those exchanges happen internally within companies, and externally, with vendors and partners, with the security research community, and with the government. In many cases, those exchanges are impromptu and ad hoc and stem from emerging security issues or discoveries, such as a script that a security researcher may write to help assess a new piece of malware. Therefore, whether internal or external, the proposed regulation could require a license for exchanges that the legislation had intended to encourage and accelerate.

What's more, as emphasized by the legislation, a significant trend in information sharing is automation and sharing in real-time, at machine speed. That type of sharing could similarly be impacted when the data is shared across national borders or shared domestically with persons from outside the United States. Administration policy as stated in Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing, promotes information sharing, as do Congress's recent cybersecurity achievements, but the proposed intrusion software definition and its implementation could have a chilling effect on reaching Congress's goals.

e. *Global Challenges Arising out of Wassenaar Implementation*

One of the challenges Microsoft faces as a company with software developers in a number of countries is that Microsoft needs to be able to comply with a range of export control regimes. Many governments have been watching the rollout of the US approach with interest. The United Kingdom's approach also requires licensing[14] and is problematic in that it, too, struggles with the same overbreadth of the underlying definition of intrusion software. While the UK's license exceptions are broader, it remains our view that a large number of licenses may be required to comply with the UK regime. We are continuing to assess the guidance. Other nations have not yet published specific guidance on how to comply with the intrusion software obligations. Some governments have expressed concern about the recent Wassenaar action, including India, which convened senior government officials to review the impact of the potential regulation for Indian companies.[15]

The United States should take a leadership role on cybersecurity issues in the export control space and work with the international community to develop a more narrowly-tailored and outcome-focused approach, rather than leave the current approach in place.

3. The Public Private Partnership and Cybersecurity Regulation

---

[14] "Notice to Exporters 2015/24: ECO issues guidance on intrusion software controls," Department for Business, Innovation & Skills, August 10, 2015, available at: http://blogs.bis.gov.uk/exportcontrol/uncategorized/eco-issues-guidance-on-intrusion-software-controls/.

[15] "Indian Officials see cyber threats from Wassenaar Arrangement", The Economic Times, June 19, 2014, available at: http://articles.economictimes.indiatimes.com/2014-06-19/news/50711034_1_cyber-threats-inter-ministerial-panel-software-products.

The "Public Private Partnership" is one of the foundational principles of cybersecurity in the United States. It has been cited in countless speeches by Government and private sector representatives at all levels, and is recognized as essential to creating smart regulatory and technical responses to cybersecurity challenges. The pubic private partnership is also important to ensure that information is shared, threats assessed, and critical issues mitigated before attacks or consequences can disrupt key services.

a. Wassenaar Arrangement Proposals and the Public Private Partnership in the US

The negotiation of Wassenaar proposals typically begins with a proposal from a member state. In the United States, there are a number of advisory committees hosted by the Department of Commerce that are used to help formulate a private sector view on the proposals before US Government representatives go to Wassenaar meetings to negotiate with the other member states.

In this case, the intrusion software proposal appears to have originated with the United Kingdom, which was seeking to control sophisticated surveillance software such as those sold by the UK company Gamma International (maker of FinFisher), and the Italian company Hacking Team, as products from those companies had been identified in attacks against "political dissidents and other activists."[16] In assessing the outcome of the Wassenaar process, however, one leading technology association noted, "Unfortunately, the negotiators of these provisions lacked technical expertise and defined 'intrusion software' far too broadly."[17]

Once the Proposed Rule reached the security community in May 2015, it was immediately clear to industry that what was agreed upon in December 2013 was unworkable.

b. The Public Private Partnership, Cybersecurity and Export Control

Fortunately, the US has a good track record overall of Congress, the private sector and the Executive Branch working together in many areas to solve difficult problems, including those involving both cybersecurity and export control. We submit that the scope of controls related to intrusion software needs to be reconsidered, and there needs to be a plan for ongoing private sector consultation as the revision of these controls is pursued. In addition, we continue to hear that issues beyond intrusion software are looming in the not-so-distant future for Wassenaar consideration. Working with our colleagues in industry, the Congress and the Executive Branch, we should be able to have a robust process in place that can address security interests without impacting security or impeding innovation.

4. Cybersecurity and Changing Global Norms

---

[16] "The Wassenaar Arrangement: Overview," BSA, the Software Alliance, (BSA Overview) available at: http://www.bsa.org/~/media/Files/Policy/IssueBriefs/12072015Wassenaar.pdf; *see also*, "Hacking Team sold Spyware to 21 Countries; Targeting Journalists and Human Rights Activists," Swati Khandelwal, The Hacker News, February 24, 2014, available at: http://thehackernews.com/2014/02/hacking-team-sold-spyware-to-21.html; *see also* "Ethopia: Hacking Team Lax on Evidence of Abuse – Human Rights Watch," Ethiopian Team, August 15, 2015, available at: http://ethiopianteam.net/ethiopia-hacking-team-lax-on-evidence-of-abuse-human-rights-watch/.

[17] *See* BSA Overview at 12.

One of the issues that has been brought to the surface through both the intrusion software discussion and the disclosure of the emails of Hacking Team is that governments, including those who may seek to suppress dissent, are often the customers of the technologies at issue here.[18] What is also clear is that different governments, including various Wassenaar signatories, will use technology and tools in ways that the United States and other nations find unacceptable, and that while some states agree on the need for export control of surveillance software, others find its use acceptable.

This issue of the use of surveillance software may be appropriate for analysis along the lines of the cybersecurity norms debate. Microsoft has observed five important principles that should underlie international discussions of cybersecurity norms: harmonization, risk reduction, transparency, proportionality, and collaboration. "These principles are important to keep in mind when governments are discussing which issues of cybersecurity rise to the level of normative behavior, which require conventions among a large number of states, or smaller, bilateral or multilateral agreements, or which are simply adopted into domestic laws or public policies."[19]

We believe that applying the principles of the cybersecurity norms debate to surveillance software and potentially other issues arising in export control of cybersecurity is that it helps ensure agreement and understanding among governments and the private sector.

> Our goal – albeit ambitious – is to prevent the emergence of a world where cyber conflict undermines trust. The alternative is to realize too late, among the wreckage, that something should have been done long ago. Cybersecurity norms that limit potential conflict in cyberspace are likely to bring greater predictability, stability and security to the international community.[20]

5. Conclusion

Microsoft welcomes the Subcommittees' interest in this matter and their oversight and guidance on how the public private partnership can continue to help advance the state of cybersecurity in the United States. We believe that this important issue is a bellwether for future cybersecurity activity, and it is important that the US demonstrates clear and principled leadership as we contemplate future regulation impacting cybersecurity.

---

[18] "Hacking Team hacked: firm sold spying tools to repressive regimes, documents claim", Alex Hern, The Guardian, July 6, 2015, available at: http://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim (noting that "if genuine, Hacking Team's clients are the governments and security services of Azerbaijan, Kazakhstan, Uzbekistan, Russia, Bahrain, Saudi Arabia and the UAE, many of whom have been criticized by international human rights organizations for their aggressive surveillance of citizens, activists, and journalists both domestically and overseas.")

[19] "Five Principles for Shaping Cybersecurity Norms," Microsoft, available at: file:///C:/Users/cgoodwin/Downloads/Five_Principles_Norms%20(1).pdf.

[20] "Proposed Cybersecurity Norms to Reduce Conflict in an Internet-dependent World," Paul Nicholas, Cyber Trust Blog, December 3, 2014, available at: http://blogs.microsoft.com/cybertrust/2014/12/03/proposed-cybersecurity-norms/.

Mr. RATCLIFFE. Thank you, Ms. Goodwin. The chair now recognizes the very patient Mr. Garfield for his opening statement.

STATEMENT OF DEAN C. GARFIELD

Mr. GARFIELD. Chairman Ratcliffe, Chairman Hurd, Ranking Member Kelly, Ranking Member Richmond, members of the committee, on behalf of 64 of the most dynamic and innovative companies in the world, some of whom are also at this table, we thank you for hosting this hearing, inviting us to testify, and for your bipartisan approach on this issue, including the letter that you sent at the end of last year. I've listened carefully to the testimony of the other folks on this panel, and rather than repeating what they've already said so eloquently, I'll try to focus in on some of the questions that were implicit in your testimony, including why is this important? What should we do about Wassenaar? Can we simply revise the rules? And what are our recommendations or next step?

As to the first, why is this important, our company, the companies that are members of ITI, are really the technology platform for the entire world. There is no sector or industry that's exempted from the implications of the Wassenaar Arrangement. Increasingly, cross-border data flows are the steam of the economic engine worldwide as well as innovation, the innovation ecosystem. The Wassenaar Arrangement impacts all businesses, whether they are technology-based or otherwise.

Can the defects in the rules be cured? Our recommendation and answer is no. In spite of the best intentions of the drafters, the fundamental flaws in the proposed rules emanate from the arrangement itself. And I'll point to three areas that are—that speak to that.

One, the presumptions, the problematic presumptions, around drawing lines between intrusion software, as well as drawing lines around IP network surveillance systems are found in the rules themselves, but are very much, in fact, grounded in the Wassenaar Arrangement as developed in 2013.

Secondly, the question that Chairman Hurd raised and Ranking Member Kelly alluded to around whether you can actually deal with the fast-paced world of cybersecurity in cross-border data flows through the lumbering world that is limited by borders in export controls, the answer is no.

Third, what is really needed here is a multinational approach, as a number of the members on this panel and the committee have noted, given the nature of our economy today, its heavy reliance on cross-border data flows, as well as the nature of cybersecurity that's been advanced by the work of this Congress through the Cybersecurity Act of 2015, as well as the Department of Commerce through NIST.

Increasingly, the way to deal with cybersecurity issues is on a multinational basis through the sharing of cyber threat information. The Wassenaar Arrangement stands in the way of that.

Relatedly, there are a number of nations that are a critical part of advancing cybersecurity that are not a part of the Wassenaar Arrangement, including Brazil, India, and China. So what do we

do? Our recommendation is consistent with the private sector witnesses on this panel. Given that the root of the challenge is grounded in the 2013 developments in Wassenaar and the Wassenaar Arrangement, our recommendation is to go back to Wassenaar to cure those fatal defects. We say that not out of taking any pride in suggesting that the United States go back and renegotiate this agreement, but from our perspective, it's truly an opportunity to exercise leadership.

There are a number of countries that are struggling with dealing with these same issues, and the United States has an opportunity to provide global leadership in dealing with what are truly complex issues.

Secondly, it's important that whatever is done next is informed by experts, including many of those that are in this room, and some of who are not.

I thank the committee, again, for this opportunity to testify. And I look forward to your questions and to working with you towards a solution. Thank you.

[Prepared statement of Mr. Garfield follows:]

Written Testimony of
Dean C. Garfield
President & CEO, Information Technology Industry Council (ITI)

Before the
Subcommittee on Information Technology
Committee on Oversight and Government Reform

And

Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
Committee on Homeland Security
U.S. House of Representatives

Wassenaar: Cybersecurity and Export Control

January 12, 2016

Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, Ranking Member Richmond, and members of the subcommittees, thank you for the opportunity to testify today. I am Dean Garfield, President and CEO of the Information Technology Industry Council (ITI), and I am pleased to testify before your subcommittees today on the important topic of the Wassenaar Arrangement and the implications for cybersecurity of imposing stricter export controls pursuant to the Bureau of Industry and Security's (BIS') proposed rule, *Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items*, released in the *Federal Register* on May 20, 2015 (the "Proposed Rule").[1] While we strongly support the Wassenaar Arrangement's human rights objectives of addressing the export and proliferation of weaponized malicious software, we have significant concerns regarding the commercial and security implications of this proposed means of achieving them. We welcome your interest and engagement on this subject.

ITI is the global voice of the tech sector. We are the premier advocate and thought leader in the United States and around the world for the information and communications technology (ICT) industry, and this year we are pleased to be commemorating our centennial. ITI's members comprise leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, Internet companies, and companies using technology to fundamentally evolve their businesses. Cybersecurity is critical to our members' success—the protection of our customers, our brands, and our intellectual property is an essential component of our business, and affects our ability to grow and innovate in the future. Consequently, ITI has been a leading voice in advocating effective approaches to cybersecurity, both domestically and globally.

Cybersecurity is rightly a priority for governments and our industry, and we share a common goal of improving cybersecurity. Further, our members are global companies, doing business in countries

[1] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853 (proposed May 20, 2015), *available at* https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

around the world. Most service the global market via complex supply chains in which products are developed, made, and assembled in multiple countries across the globe, servicing customers that typically span the full range of global industry sectors, such as banking and energy. As a result, we acutely understand the impact of governments' policies on security innovation and the need for U.S. policies to be compatible with – and drive – global norms, as well as the potential impacts on our customers. As both producers and users of cybersecurity products and services, our members have extensive experience working with governments around the world on cybersecurity policy. In the technology industry, as well as banking, energy and other global sectors, when discussing any cybersecurity policy, it is important to consider our connectedness, which is truly global and borderless.

I will focus my testimony on four areas: (1) The critical importance of cross-border data flows to cybersecurity; (2) the potential impacts of the Proposed Rule and the Wassenaar Arrangement 2013 Plenary Agreement on our companies' cybersecurity and innovation efforts; (3) the broader effects of the Proposed Rule and the Wassenaar Arrangement 2013 Plenary Agreement on ecosystem cybersecurity for all industries; and (4) recommendations on how to best achieve the objectives of the Wassenaar Arrangement without compromising security objectives.

Cross-Border Data Flows and Cybersecurity

A central element of ITI's global advocacy efforts involves helping governments understand the critical importance of cross-border data flows, not only to the ICT sector, but also to the global economy as a whole. Virtually every business that operates internationally relies instinctively on the free and near instantaneous movement of data across borders to enable their day-to-day business operations, from conducting research and development, to designing and manufacturing goods, to marketing and distributing products and services to their customers. U.S. and global ICT companies also have a long history of exchanging security-related information across borders with geographically-dispersed employees, users, customers, governments, and other stakeholders, which helps them protect their own systems and maintain high levels of security for the technology ecosystem as a whole.

Indeed, as well as facilitating secure business transactions amongst companies in disparate locales, global data flows are key to greater coordination and productivity for companies globally, helping to secure the systems and networks that manage production schedules and Human Resource (HR) data, as well as communicate internally with subsidiaries and employees in different geographies. The free flow of data across borders is necessary to enable a seamless and secure Internet experience for hundreds of millions of citizens around the globe. The Proposed Rule is part of a troubling global trend of erecting barriers to the free movement of global data, as also exemplified in the recent European court of Justice opinion effectively invalidating the Safe Harbor agreement.

Perhaps even more disturbing, the Proposed Rule, and the trend of impeding data flows generally, is contrary to the thrust of current U.S., and indeed global, cybersecurity policy.

To illustrate, as you know, late last year, Congress passed a bipartisan cybersecurity threat information sharing bill, the Cybersecurity Act of 2015.[2] The bill acknowledges that voluntary sharing of information

[2] Consolidated Appropriations Act, 2016, H.R. 2029, 114th Cong., Division N (2015).

regarding cyber threats, with appropriate privacy safeguards, is an integral component of improving our cybersecurity ecosystem, as it helps all stakeholders better protect and defend cyberspace. More specifically, Section 103 requires the heads of various federal security agencies to jointly develop procedures to ensure the Federal Government maintains "a real-time sharing capability." Section 105 directs the Attorney General and Secretary of Homeland Security to jointly develop policies and procedures to govern how the Federal Government receives and shares information about cyber threats, including via an automated real-time process, and Section 203 requires the Department of Homeland Security, in coordination with industry and other stakeholders, to develop an automated capability for the timely sharing of cyber threat indicators and defensive measures. President Obama signed the law, which aligns with the Administration's consistent recognition of the critical importance of cross-border data flows and real-time information sharing in combatting security threats to the global ICT environment. For instance, also last year, President Obama issued Executive Order 13691,[3] which, among other things, states, "private companies, nonprofit organizations, executive departments and agencies, and other entities must be able to share information related to cybersecurity risks and incidents and collaborate to respond in as close to real time as possible."

All of these policy efforts are intended to spur the voluntary sharing of cyber threat information among and between businesses and government entities to improve cybersecurity, and all of these initiatives contemplate the sharing of cybersecurity threat information as inclusive of information related to vulnerabilities. Given that the overarching intention of these policy initiatives is to promote expedited sharing of threat information to improve cybersecurity, we are concerned that the Proposed Rule and the 2013 additions to the Wassenaar Arrangement could undermine this key principle and severely complicate the ability of companies in all sectors and government entities to share information in real-time to protect and enhance their security.

The onerous licensing scheme contemplated by the Proposed Rule, however, would necessarily slow down the sharing of vulnerability information (both intra-company and between companies). In other words, because the Proposed Rule is effectively erecting additional barriers to vulnerability sharing, it appears diametrically opposed to the goals of multiple cybersecurity policy initiatives recently advanced by U.S. government policymakers.

Potential Impacts of the Proposed Rule on Tech Sector Innovation and Cybersecurity Efforts

The Proposed Rule would significantly damage cybersecurity technology innovation efforts by burdening companies with the onerous and time consuming process of applying for large volumes of unnecessary licenses. The damage could potentially impact a wide range of cybersecurity products and technologies in development, such as innovative defensive cybersecurity products, in addition to potentially restricting research into cyber vulnerabilities and exploits connected to valuable internal business activities, such as research and testing to determine vulnerabilities in our companies' systems, products and technologies. Both of these sets of activities are intended to strengthen the cyber defenses of our companies and customers worldwide. At a minimum, the licensing scheme envisioned by the Proposed Rule would negatively impact the ability of companies in the U.S. seeking to develop such tools, and

[3] Exec. Order No. 13,691, 80 Fed. Reg. 9347 (February 20, 2015), *available at* https://www.federalregister.gov/articles/2015/02/20/2015-03714/promoting-private-sector-cybersecurity-information-sharing.

would almost certainly leave critical data systems much less protected, and subject to increased cyberattacks or breaches by malicious actors, because of the inevitability of delays associated with applying for and receiving approvals for license applications.

As an initial matter, the Proposed Rule presumes clear lines of demarcation between "intrusion software" (not controlled), and "software that generates, delivers, or communicates with intrusion software" (controlled). However, subject matter experts do not agree on whether this line actually exists, and if it does, exactly where it lies. The natural consequence for compliance-driven exporters would be to assume a very conservative position by "playing it safe" and assuming that large volumes of software or technology would be controlled. The natural consequence for BIS would be unpredictable (but likely large) volumes of license applications.

Similarly, the overall breadth of the draft measure would mean that companies could be required to apply for and obtain literally thousands of export licenses to cover the vast range of information-sharing and other security-related activities that they undertake involving the movement of data across borders (in areas such as product development, security testing and research) and the proper securing of their own and their clients' information and networks. It would be extremely burdensome and costly for both individual companies to prepare license applications as well as for BIS to review and rule on them. It would also be extraordinarily time consuming. Months could pass between the time the need to share threat information arises and the time permission to do so is granted. Meanwhile, potential vulnerabilities could be exploited many times over.

The Proposed Rule would be harmful to individual companies as it relates to their own internal data sharing and cybersecurity operations. A single company might need to obtain large numbers of licenses for its headquarters to share certain security information, software and tools with overseas affiliates or use certain products to insure the security of its internal network. Even domestically, a manager at headquarters might need to obtain a license to walk down the hall and discuss certain security issues or development of new tools with a team member who is a national of a country other than the United States or Canada.

While concerning for any company doing business globally, the problems would disproportionately impact many companies in the tech sector, particularly companies developing software deployed across industry networks and the cloud, and security companies working to innovate solutions to help protect all stakeholders' networks and systems.

Also troubling for these companies is language in the Proposed Rule empowering BIS to make the granting of licenses contingent upon companies' disclosing their source code. The Proposed Rule states, "when an export license application is filed, BIS can request a copy of the part of the software or source code that implements the controlled cybersecurity functionality." We strongly urge BIS to reconsider any requirement that applicants hand over their source code. This is particularly important at a time when U.S. officials and industry are urging foreign governments not to compel vendors to turn over intellectual property, such as source code and other sensitive corporate data.

Broader Impacts of the Proposed Rule on Cybersecurity across Industry

Concerns regarding the Proposed Rule do not only impact the technology sector – they will negatively impact the ability of all companies to defend themselves from cybersecurity threats. All sectors, especially critical infrastructure, need effective cybersecurity, including the ability to share information quickly within sectors, among other sectors and with the Federal government, to discover and close vulnerabilities before they are widely known.

To be able to detect and remediate vulnerabilities – whether in products or systems – companies must retain the ability to identify and test those vulnerabilities. Even products that are not "specially designed" to perform the single intrusion function may be captured under the breadth of the Proposed Rule.

Most fundamentally, the Proposed Rule would do more to damage, rather than improve, the cybersecurity of U.S. companies, by restricting access to protective security measures required by networks all around the world. Imposing significant constraints on the ability of multinational corporations across multiple sectors to take cyber self-defense actions seems to belie common sense. For instance, companies' vulnerability assessment teams use "intrusion software" to identify and track vulnerabilities in network devices and applications. The ability of companies to perform this activity across global boundaries, by sharing vulnerability information amongst their own-geographically dispersed or multi-national employees, should not be impeded.

Collaboration is most urgently needed during ongoing attacks. As stated above, the entire point of passing information sharing legislation was to facilitate the sharing of cybersecurity threat information, including information regarding security vulnerabilities, in as close to "real time" as possible so as to more quickly remediate them and minimize potential damage to companies' networks. Potentially high-risk vulnerabilities are most valuable to hackers, and so are the exact type of cyber weaknesses that companies want to find during their internal penetration testing. Injecting a licensing scheme, with onerous requirements precluding intra-company transfers of critical cybersecurity threat information that would prevent companies from taking necessary defensive actions across their worldwide networks, seems to make little sense.

This problem is exacerbated by the Proposed Rule's "policy of presumptive denial" for zero-day and rootkit capabilities, e.g., "product or system" or "delivery tool."[4] Presumptive denial would greatly restrict businesses' abilities to share threat information and counter some of the most dangerous cyber vulnerabilities and exploits. Detailed technical data on the origins of a previously unknown vulnerabilities, or zero-days, is the very same information that enables bad actors to exploit weaknesses in companies' computer systems. If there is no technical difference defined in the Proposed Rule between the cybersecurity activities performed by our companies and the criminal activities performed by hackers, our companies will be significantly hampered by the imposed controls.

[4] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853, 28855 (proposed May 20, 2015), *available at* https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

For the same reasons, the proposed export control regime could also impose severe limitations on information sharing beyond the walls of companies themselves, impacting established cybersecurity information sharing best practices more generally, including sharing within public-private partnerships (e.g., sector-coordinating councils and information-sharing and analysis organizations), and sharing linked to government contracts and protected programs. For example, information that is shared with the U.S. government voluntarily (e.g., US-CERT) or as required under contracts (e.g., FISMA and FedRAMP) could be thrown into question, which would benefit neither the government nor the private contractor.

Additionally, the portions of the Proposed Rule restricting surveillance items might also impact established best cybersecurity practices of companies. For instance, many companies utilize some type of packet analyzer (i.e. packet sniffer) to monitor and capture digital traffic passing over a network so that technicians can identify malicious code. The 2013 amendments to the Wassenaar Arrangement added the following to the list of dual-use goods: "Internet Protocol (IP) network communications surveillance systems or equipment and test, inspection, production equipment, specially designed components therefor, and development and production software and technology therefor."[5]

It is unclear how the inclusion of the restriction regarding IP network communications might impact the ability of companies to deploy their monitoring equipment and software in multiple locations on their networks to fight bad actors. Imposing licensing requirements that could impact such smart and basic cybersecurity practices seems both unfeasible and detrimental to enterprise security.

Recommendations

The Proposed Rule raises a host of complex and interrelated technical policy issues involving usually disparate topics including cybersecurity, export control law, and human rights, and impacts government and industry interests alike. Given the diversity of impacted and knowledgeable stakeholders in these divergent areas, public-private collaboration in this issue area would greatly enhance the expertise of federal government representatives both at Wassenaar and in any future rulemakings.

Thus, at a minimum, we urge BIS to withhold publication of the Proposed Rule, and forgo further revisions with an eye toward implementation, and to instead engage the U.S. ICT industry, its inter-agency partners, and other stakeholders in detailed consultations regarding how best to achieve the objectives of the Wassenaar Arrangement without compromising the security objectives of both the Administration and the ICT industry. Such consultations would allow government and industry to discuss options and what further steps to take (likely in parallel) including, but not limited to:

- Returning to Wassenaar to reopen the control, and in the interim, withholding the rule from publication. Renegotiating the agreement is certainly a better option than simply not implementing the rule, which seems neither a prudent nor practical option. However, given that there appears to be wide variation amongst Wassenaar signatories in the implementation

[5] Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance, 80 Fed. Reg. 28853, 28854 (proposed May 20, 2015), *available at* https://www.federalregister.gov/articles/2015/05/20/2015-11642/wassenaar-arrangement-2013-plenary-agreements-implementation-intrusion-and-surveillance-items.

of the particular provisions impacting cybersecurity, clarifying the Wassenaar Agreement language itself seems the surest means of ensuring consistent implementation in a global cybersecurity environment.

- Establishing a working group of technical experts from government and industry to systematically address both the technical and policy aspects of the cybersecurity, human rights and export controls considerations at issue. As stated above, the Proposed Rule implicates competing equities and impacts multiple stakeholders. With this is mind, we call for the formation of an experts group to represent these competing interests and fully analyze the multiple facets of implementation of the 2013 Wassenaar Arrangement Plenary Agreement. We believe the experts group should have a broad charter and could examine any number of topics, including:
    - *Options for targeted implementation.* If reopening the control at Wassenaar proves unsuccessful and the U.S. has no choice but to implement the Proposed Rule, it is essential to work with security experts from government agencies and industry to devise an appropriate, targeted solution in consideration of all the dimensions of this important issue, so as to minimize the broader impacts. In particular, we advise examining how to limit the scope and coverage of the Proposed Rule via a narrower definition to avoid disrupting day-to-day business and security operations of global companies.
    - *Applicability of Pre-Existing Rules.* The experts group might explore whether any pre-existing rules might be applicable, or able to be modified, to address some of the legitimate human rights concerns underlying the rule.
    - *Targeting Bad Actors.* Exploring whether there is a way to target bad actors, as opposed to the current approach, which targets the technology. The experts group could focus on the variance between "defensive" and "offensive" cybersecurity measures, in an effort to differentiate between "white hat" developers who are seeking to improve security across the ecosystem and "black hat" hackers who are focused on substantially harming an information system or data on an information system. Enabling BIS to set appropriate export controls based on malicious end use which do not inadvertently subject companies, researchers and others to burdensome and onerous internal licensing requirements in order to conduct day-to-day business would be a win.

Conclusion

Members of the subcommittees, ITI and our member companies are pleased you are examining how the Wassenaar Arrangement will affect the cybersecurity of our nation and private industry. The ICT sector is innovative and dynamic, continuously evolving as new products are developed and existing technologies are improved. However, the threats to our security also constantly change. Criminals and other bad actors modify and adapt their techniques almost as quickly as the industry is constantly innovating to address those threats. However, for our security efforts, and those of the federal government, to be effective, any cybersecurity regime implemented by government bodies must be flexible to allow government and private industry systems to leverage new technologies and business models, address constantly changing threat dynamics and manage new risks and vulnerabilities.

In addition, there are potentially broader international ramifications of pursuing policy approaches such as those embodied by the Proposed Rule. Whatever the rationale, the broad scope of the Proposed Rule could be viewed as the imposition of government restrictions on cross-border data flows. Such rules would provide a precedent for other governments to expand their own limitations on the flow of information across borders, including on the basis of "security," to the detriment of global trade and U.S. companies operating in those markets. Doing so would not only impose tremendous costs on some of the United States' leading innovators and job-creators, but it would also directly undermine efforts to achieve the Administration's objectives for enhancing commercial information security, both of the companies covered by the regime and the global ICT ecosystem generally.

We stand ready to provide you any additional input and assistance in our collaborative efforts to develop balanced policy approaches that help all of us to achieve the objectives underlying the Wassenaar Arrangement while also collectively improving cybersecurity innovation, risk management, and resilience.

Thank you.

Mr. RATCLIFFE. Thank you, Mr. Garfield.

The chair now recognizes himself for 5 minutes of questions.

And I want to start, Ms. Ganzer, with you, because you were the only witness that didn't have a statement, and there was some intimation about—about your role, perhaps, in negotiating the Wassenaar Arrangement of 2013 and the inclusion of intrusion software. And so I want to take just a minute of my time to give you an opportunity to address whether or not that's accurate, or what your role was, if any?

Ms. GANZER. Thank you, Mr. Chairman. I appreciate the opportunity to be here today. In my role as the Director of Conventional Arms Threat Reduction, I am the head of delegation for the Wassenaar Arrangement writ large for the United States. So I was in the chair for the United States when the control was adopted and agreed to on behalf of the United States. I was not responsible, specifically, in the room when it was negotiated. The administration has an integrated team of members from the interagency generally, including the Commerce and Defense Departments; Homeland Security may be there; Energy may be there; depending on what issue is being negotiated. But the administration and an integrated team negotiated these controls. And, so, there would have been an integrated team that agreed to the specifics.

I would note that the control was intended to capture purpose-built suites of operated control—operator controlled software that extract—are designed to extract data from a system, modify a system or its data, or modify the system to execute a malicious operator's instructions without the systems owner's knowledge. That was what we intended to control, and that is what we thought we controlled. So the reaction from our industry colleagues here was quite a prize to us. And we continue to work the issue within the administration to—to do no harm, as some of the members mentioned in their statements. Thank you.

Mr. RATCLIFFE. Terrific. Thank you. That's helpful, Ms. Ganzer.

So based on that, and you answered my next question, was based on the comments you heard today and the more than 300 formal comments from industry, were you surprised? And you said that you were.

As a follow-up to that, do you think those comments are justified?

Ms. GANZER. Sir, the industry knows what they are doing. So, absolutely. Many of the comments were very serious, went into very detailed analysis of the proposed rule, many proposed exceptions or different ways that we could address some of their concerns, and many of them were amplified, or reiterated through the process of meetings that the Department of Commerce hosted, in which I and several members of my team attended to listen to these concerns from industry.

So, absolutely, they—they were, in many cases, right on the mark, and we are taking them very seriously.

Mr. RATCLIFFE. Terrific. Thank you.

So let me follow up on the specifics. One of the comments, I believe, was from Ms. McGuire and others in the industry, as drafted, what keeps bad actors that the Wassenaar Arrangement is seeking

to stop from purchasing unlicensed products, or purchasing products in a nonparticipating state?

Ms. GANZER. Thank you for that question. That's a difficult one to answer. As Mr. Van Diepen has already indicated, export controls are most effective when they are multilateral. And so this is why we work through organizations like the Wassenaar Arrangement when we establish controls, because, first of all, 41 members of the Wassenaar Arrangement, including many of our allies who developed this sophisticated technology, commit to the controls in the Wassenaar Arrangement, and there are a number of other countries that unilaterally adhere to the Wassenaar Arrangement controls.

So we do capture a good portion of the market by establishing controls in a multilateral form like the Wassenaar Arrangement.

Mr. RATCLIFFE. Okay. Well, I appreciate that.

Do you think, or would you agree, that as written, there's a security consequence to the domestic implementation of the Wassenaar Agreement as some folks in industry have indicated?

Ms. GANZER. It—just to clarify, it was a proposed rule. Nothing has actually been implemented yet. But indeed, since we did not intend to capture many of the scenarios that were—were presented to us by industry, this is something that we need to fix, and we are working interagency, analyzing the comments, following up with them to determine what our next steps forward will be.

Mr. RATCLIFFE. So I appreciate that.

So as my time expires, in terms of coming to that solution, you've heard some calls here from folks in industry for this to be renegotiated. And so my question to you is, why or what are the impediments, if any, to doing that? Because as I was understanding the arrangement, it meets every year.

Ms. GANZER. Well, first and foremost, we have not yet determined whether we need to do that. The interagency continues to work that issue. So saying we are going to go back and negotiate would be premature. But I would note that the Wassenaar Arrangement operates by consensus. All 41 members will have to agree, and 31 members have already implemented this control. So that is—we are also looking at how other countries are controlling this or have implemented it, and that will all be taken into account in the administration's decision on what we will do going forward when we—when we get there.

Mr. RATCLIFFE. Terrific. Thank you, Ms. Ganzer.

My time has expired. The chair now recognizes the ranking member, Ms. Kelly, for her questions.

Ms. KELLY. Thank you, Mr. Chair.

As I stated in my opening statement, today's hearing is a recognition of the fact that the Federal Government and the private sector must work together effectively to thwart cybercrime and to support advancement in cyber defense and research.

Mr. Garfield, you talked about meeting a multinational approach, sharing information, curing fatal defects, exercising leadership, and that leadership that we exercise needs to be informed by experts.

What role do you see that Congress can play to ensure that the private sector's concerns pertaining to the proposed Wassenaar regulations are adequately addressed?

Mr. GARFIELD. Thank you for listening so carefully. You've recounted my testimony more effectively than I did.

I think the thing you can do you are, in fact, doing. So the letter that was sent in December making sure that there's a recognition that this is not political, it's bipartisan, and it's critically important. I think the second thing is, in fact, Congress insisting on getting real answers on what's going to happen next. And so continuing your oversight, I think, is an important part of the role that you can play in this area.

You've done a lot through the bills that you've passed on cybersecurity, including the Cybersecurity Act of 2015, and we commend you for that.

Ms. KELLY. Thank you. This rulemaking is an opportunity for the government and private sector to demonstrate that working together can produce positive results with no unintended collateral harm to cyber's defense capabilities.

Ms. Goodwin, one area of your testimony focuses on the importance of the public-private partnership in cyber security regulation. I was wondering if you could, if possible, offer examples of private-public partnerships in cybersecurity that are working, and that could serve as an example for how the implementation of the Wassenaar Arrangement export controls might be revised to meet the government and private sector?

Ms. GOODWIN. Thank you, Ranking Member Kelly. There are a number of things that we can point to in the public-private partnership space. The collaboration and coordination that the private sector and companies like Microsoft has with the Department of Homeland Security's Computer Emergence Response Team, U.S. CERT, its collaborative way in which it comes together to triage incidents that the security community's conferences and hacking competitions and prizes to find the best way to disassemble the vacuum cleaner and put it back together, this is a robust community where the ability to exchange information with the government and with other companies is absolutely essential to our ability to secure ourselves and our customers.

Imagine if Congress were to pass a bill without any constituent input, without any consultation with experts, and then once the bill had been signed into law, then to say, well, we'll work on the implementation after the fact. The reality is that we have a very robust public-private partnership that we'll have to leverage. In the event that additional export control ideas are floated in a community where the private sector may not play, we have to rely on our government partners to bring this to us and to triage them and to think about the implications and consequences before we take any position.

This—Mr. Wolf said that this was an issue of first instance in his testimony. We had not attempted to tackle cybersecurity quite like this in the export control space, so this is an opportunity for us to rethink the process so that the public-private partnership can be brought to bear in these types of questions, so that we don't have to, like you said, to regulate first and ask questions later.

Ms. KELLY. Thank you.

Mr. Mulholland, as the engineer on the panel, do you think it would be sufficient that the administration, through a revised policy, puts in intracompany license exemption into a new rule?

Mr. MULHOLLAND. Thank you, Congresswoman Kelly, for the question. The simple answer to that is no. The reality is that might help our situation domestically, but the reality is, is that as a global company, I will seek threat information on my products from anywhere.

You know, we heard a few minutes ago that there are 31 countries have already implemented Wassenaar. The reality is, in my mind anyway, Wassenaar is not 41 countries in this space, it is 40 plus one. There is one country in this world and one country and not 41 who provides overwhelming leadership in the technology sector. The reason why I don't think we've actually seen any negative consequences from the other 31 is because, frankly, their expert ratings are not likely to be injurious to their industries, because, frankly, they don't have particularly vibrant industries.

And I, you know, heard many of the members have commented on our leadership. Ms. McGuire cited an example where a U.S. company pulled out of Japan, pulled out of participating in a very long, established security research conference in Japan. Does that injure Japan's technology industry, or does it injure the U.S. industry? My vote is that it injures the U.S.

So in short, no, BIS fixing the situation here in the U.S. does not fix the problem. The only way the problem gets fixed is to go back to Wassenaar, or perhaps, even concerning whether export controls is the right way to tackle this problem.

Ms. KELLY. Thank you. And I'm out of time.

Mr. RATCLIFFE. I thank the gentlelady.

At this time, I ask unanimous consent to insert into the record a letter from more than 100 Members of Congress to Ambassador Susan Rice regarding our collective concerns about the addition to the Wassenaar Arrangement to export controls of intrusion software that, in our opinion, could seriously hinder national security.

Without objection, it is so ordered.

Mr. RATCLIFFE. At this time, the chair recognizes my friend and colleague from Texas, Congressman Farenthold.

Mr. FARENTHOLD. Thank you very much, Mr. Chairman.

And I wanted to start out with Ms. Goodwin from Microsoft. We've talked a little bit about, today, about how some of this software is available from countries that aren't a party to our agreement. I know Microsoft is active in fighting software piracy as well. Even in the domestic, international stuff that we're seeking to regulate, software is pretty portable and pretty easy to pirate. Do you think there's a practical way we can actually put export control on software against, obviously, a hacker who would be typically unethical to begin with, or a state actor that's hostile to us? I imagine y'all struggle pretty hard from keeping Microsoft Word from getting pirated?

Ms. GOODWIN. That's a great question, Representative. Not only is it a challenge from a piracy standpoint, it's also a challenge from a legal standpoint. If you look at the implementation of the Wassenaar Arrangement thus far, I would point to the hacking team, which is a company that creates this type of intrusion soft-

ware, and over in the gov—in Italy. And the Italian Government issued them a license to continue to sell this software.

And when the hacking team was actually hacked itself, and its email was disclosed around the world, it was found that this software, which had been licensed by the government in Italy under this regime had been sold to regimes like Ethiopia and Sudan.

And, so, part of the challenge in thinking about how do we apply export control in the space is what do we do when you have uneven, or different implementations that software actually can be licensed, and then sold and used in ways that are contrary to the original intent of the regulation? So it is extremely difficult to figure out how to solve a challenge like that.

Mr. FARENTHOLD. Let me ask you another question. It seems like we're focusing on regulating the tools rather than the people. I mean, I think that kind of goes along the—you know, not just even the developers, but the folks that are using it. I mean, where do you—where do you see—do you think that's a better idea, and do you think that's more doable?

Ms. GOODWIN. There are criminal laws in place today that can be used to leverage to pursue those that are violating cybercrime laws. The European convention on cybercrime is a multilateral tool and instrument that we can use as well. And so what we can do is focus more on prosecution and looking at negative implications of how these tools are used. Yes, absolutely.

Mr. FARENTHOLD. Thank you very much.

And let's talk to, I guess, Ms. Ganzer from the State Department. As y'all's team was getting ready for the negotiations, did y'all go out and talk to companies like Microsoft or Symantec or VMware? What was your engagement with the industry?

Ms. GANZER. There's—thank you for the question, Congressman. There's an established process by which we share this information with the Commerce Department technical advisory committees who are made up of industry. I actually think it might be more appropriate——

Mr. FARENTHOLD. Kevin, do you want to—Mr. Wolf, you want to take that one?

Mr. WOLF. Sure. Before agreeing to or submitting a proposal to Wassenaar or any of the other regimes, we share it with one of six technical advisory committees that are all volunteers, industry participants, experts in the area. And the original idea was shared with the relevant groups, and they didn't have any objection on the thought that——

Mr. FARENTHOLD. Did it come as a surprise to you that we got so many negative comments?

Mr. WOLF. Well, by the time we received the comments, no. At the time we agreed to the control, it would have, because the original understanding was that it was a quite narrow, specific, a very small number of products that would be affected. And as we began to learn more and engage in the very industry output that is being discussed here, we began to get more and more concerned of unintended consequences, and that's why I said I think this is the first time we, Commerce, have actually pulled out from the implementation rule for a regime rule. And instead of gambling and potentially getting it wrong, went out to industry to confirm if our suspicions

were correct, or maybe we were being too concerned, and then the comments came in.

And that was actually part of the plan, was to see if we made a mistake, needed to do something differently at whatever level. So in a way, the process is actually working exactly as intended.

Mr. FARENTHOLD. Would you agree with that, Ms. Ganzer?

Ms. GANZER. Absolutely.

Mr. FARENTHOLD. And were you surprised with the comment, the number of comments as well or the——

Ms. GANZER. Much as Assistant Secretary Wolf said, by the time they came in, no. But when we first started this process, yes. Because we had thought, based on the comments from our Wassenaar partners, that we had negotiated a rather narrow control. Thank you.

Mr. FARENTHOLD. I see my time has expired.

Thank you, Mr. Chairman.

Mr. RATCLIFFE. I thank the gentleman.

The chair now recognizes the gentlelady from California, Ms. Sanchez.

Ms. SANCHEZ. Thank you, Mr. Chairman.

And it's fascinating. Every time I come to a cyber issue, it's just incredibly fascinating. I remember—I'm from California, so, of course, we think that we have encryption and cyber as far cutting edge as possible.

I remember, Mr. Chairman, 20 years ago, when I sat on the Armed Services Committee, we had instituted a military—a bloc on sending encryption out. And at the time, it was Adam Smith and myself were the only ones who were going, wait a minute, if we do that, we're going to lose encryption ability, or technology lead in California or the United States. And, in fact, we struggled, as Symantec and others will tell you, prior to the company, we struggled quite a bit until we were able to undo some of those restrictions.

So you were surprised, even though you had—you thought you had industry covered through the system. So my question to you would be, have you gone back and rethought different levels you might have interacted at the time with respect to that so we don't have the same type of surprise again? Because these issues of export controls and what is used and what is the standard and who's setting the standard and who's got the keys, it's going to come up over and over and over again.

So have you—have any of you gone back and rethought it, say, there might—where you could have interjected industry earlier, or was industry just sort of like, yeah, yeah, yeah? Sometimes that happens here in the Congress. You know, someone comes up to you, yeah, yeah, yeah, sign me on. Then you go back, and you think about it, and you have to pick up the phone and say, wait a minute, maybe what I agreed to isn't exactly what I was thinking at the time.

Mr. WOLF. Sure. I would cite the fact that—as I just said, we pulled out of the implementation rule this specific topic only, and instead of just implementing it, shooting first and asking questions later, as was referred to earlier, asking for industry input before deciding.

This is also highlighted the complexity of this topic in general, and we're always looking for new volunteers and participants with different areas of expertise to join our technical advisory committee. It's a volunteer organization. And so absolutely, on a going-forward basis, I plan to have more experts in this to help us review this, and to the extent this type of issue comes up in the future.

In the short term, in the meantime, we have this particular issue. And, you know, with the great benefit of our colleagues from other parts of the U.S. Government and other industry participants and the actual comments that have come in, the goal is to think through all the various options and ways to address all the various concerns that were described today to achieve the objectives, but without the harm. So the short answer to your question is yes.

Ms. SANCHEZ. Good. That's what we like to hear.

Mr. WOLF. Yes, ma'am.

Ms. SANCHEZ. Secondly, so some countries, or signatories to this, have already started to implement, as you say. And, of course, the big gorilla in the room is the United States, as you know, because we—I think, again, we still hold the edge on this area in the industry, and probably the industry itself.

So what is the process to go back and renegotiate if we've already—if some countries have already started implementing? What would we—what does Congress need to—do you need Congress involved in this? Or is it just an administrative thing where, you know, the administration could go back and say, Hey, guys, we were kidding; let's sit down; we've got to redo this?

Mr. VAN DIEPEN. Well, Congresswoman, again, we're still, as an administration, working through the comments and then the various options we have for mitigating the problems and then consulting with industry. I think one of the things we'll do as part of that is consult with the Wassenaar, or the 31-plus Wassenaar countries that have already been implementing this control for a year without apparent controversy to find out from them well, what has their experience been? Once we sort of, you know, canalize the comments, how do you guys deal with issues like this and get from them ideas that could help us?

Ms. SANCHEZ. And if that doesn't work, the reality is that we do need to renegotiate?

Mr. VAN DIEPEN. If at the end of the day, we think that we need to try to renegotiate the control, you know, then, at that point, you know, it's a diplomatic discussion amongst 41 countries. And as noted, at the end of the day, any change will require consensus. All of them would have to agree. And for a number of them, and, presumably, their starting point is going to be, Well, wait a minute, we've been implementing this control for a year plus. We haven't had any problems. Why are you guys having problems? And so we'll have to have that kind of discussion going—going back and forth. But at the end of the day, it would require us to be able to convince the other countries to go along with some sort of modification.

Ms. SANCHEZ. Great.

Mr. Chairman, thank you for the time. And let me just say that I think this is an important issue and, hopefully, we can get a timeline out of the administration about where they might be

and—so that we can make sure that we keep up with what's going on on this in case it needs to be renegotiated.

Mr. RATCLIFFE. I thank the gentlelady for her comments.

And at this time, the chair recognizes the former U.S. Attorney from Pennsylvania, my friend, Congressman Marino.

Mr. MARINO. Thank you, Chairman.

Good afternoon, ladies and gentlemen. Thank you for being here.

Ms. Ganzer, can you clarify something for me, because I was running in and out to other—other hearings.

What specifically was your role in this negotiation? Are you—were you the person that made the final decision in the Wassenaar Agreement?

Ms. GANZER. As I said, ultimately, it's my responsibility, Congressman, but, in fact, this had to be agreed across the administration. We all agreed to the control before we said okay.

Mr. MARINO. What part did—maybe Mr. Van Diepen—am I pronouncing that correctly? What part did you play in this, sir?

Mr. VAN DIEPEN. I am the Deputy Assistant Secretary supervising Ms. Ganzer's office. So among other things, would have approved the interagency guidance cable that set out the parameters of what proposals we could and could not agree to in the Wassenaar——

Mr. MARINO. Okay. Now it's starting to make sense.

Mr. Wolf and Ms. Schneck.

Mr. WOLF. No, I would like to concur. This is—all agreements with Wassenaar are as a result of consensus of the Departments of Commerce, State, and Defense. And so it wasn't just State, you know, unilaterally agreeing to it. It was the consensus of the departments participating.

And as I said, we had doubts about it later, but at the time, it was a consensus decision of the administration.

Mr. MARINO. Okay. Ms. Schneck, am I pronouncing that correctly?

Ms. SCHNECK. Schneck.

Mr. MARINO. Schneck. I'm sorry.

Ms. SCHNECK. Close enough.

Mr. MARINO. Okay. What part did Homeland Security play in this?

Ms. SCHNECK. So we provided technical insights. Our Office of Science and Technology holds our export controls portfolio, which includes Wassenaar. Where I sit, which is a different directorate, the national protection and programs directorate, provided some technical advice. We've had a challenge in finding a way to adopt export controls in a way that supports, again, our national security without affecting our homeland security cybersecurity operations that I oversee and the technology——

Mr. MARINO. Okay. Now, I heard Ms. Ganzer say that industry was consulted, and I think Mr. Wolf said industry was consulted. Is that true?

Mr. WOLF. Through the technical advisory committee process, yes, not through a proposed rule, which would have more broader industry——

Mr. MARINO. Okay. Did State do that, have that discussion with industry? Then did Commerce have that discussion with industry? And Homeland have that discussion with industry?

Mr. WOLF. No, it really wouldn't be State's process to do that. That's really the role of the Commerce Department to use its advisory committees to get industry input and then feed that out to the other departments.

Mr. MARINO. Okay. Now, you talked about, what was it, 30-some or 40-some other countries have already implemented this rule?

Ms. GANZER. 31.

Mr. MARINO. My question is, what weight is that going to carry? You know, are these other countries going to have more weight in this? Do they have a bigger dog in this fight than our own homegrown U.S. companies?

Mr. VAN DIEPEN. Congressman, I'm not sure it necessarily ends up being a weight issue. Again, we are going to have to determine——

Mr. MARINO. Well, certainly, it's going to be a weight issue, because it involves jobs here in the United States. It involves security. It involves business in this country that create tens of thousands, hundreds of thousands of jobs. And the point I'm trying to get across is, I want enough attention paid to industry here in the United States than letting someone in Europe making the determination of how we're going to play football over here.

Mr. VAN DIEPEN. Absolutely, Congressman. And what I was trying to just say is the first instance will be, do we think we can come up with a U.S. method of implementation of the Wassenaar rule that is satisfactory? If that's the case, we have the entire unilateral national discretion to implement it that way, and no one else can gainsay us. So that would be a problem.

Mr. MARINO. Now, is this a still an open, ongoing process?

Mr. WOLF. Absolutely.

Mr. MARINO. And are you going to communicate with four people at the end of the table here and others that I see in the gallery here about what is the most efficient way to do this and what is the best bang for the U.S.? Because I'm tired of us taking a back seat with this administration and worrying about what other countries want.

So are you giving us your word here that you are going to talk with these people and not be disingenuous about the meetings with these people, about what they need to continue to provide jobs here in the U.S.?

Mr. WOLF. Well, a couple—absolutely. And a couple of things. Unlike any other country, the U.S. Government went out and asked for industry comment through a proposed rule. No other government did that. We have had multiple open, public sessions with these attendees and many, many other countries to overtly, deliberately, aggressively ask their views and expertise. That process is going to continue over the course of 2016——

Mr. MARINO. Okay. I see my time has expired. I would like to see an emphasis put on what we need here in the United States. And I trust that you will do that.

And I yield back. Thank you.

Mr. RATCLIFFE. I thank the gentleman.

The chair now recognizes the gentleman from Virginia, Mr. Connolly.

Mr. CONNOLLY. Thank you, Mr. Chairman. Welcome to a very large panel.

Mr. Wolf, I want to go back to the beginning to understand the process. So the Wassenaar Arrangement involving 41 countries, a lot of those members come to us saying, will you help? We think we need some kind of expert control over cybersecurity countermeasures. Is that correct?

Mr. WOLF. That is correct, as part of the Wassenaar discussions.

Mr. CONNOLLY. Right. Right. Normally, the Wassenaar Arrangement involves things, right, defense, goods, and products?

Mr. WOLF. Well, it involves physical things, commodities, both do or use and military, but it also involves software for those things and technology for those things.

Mr. CONNOLLY. Right. Okay. All right. Would you not agree that, in the terms or—in the context of export controls, controlling things, widgets, is easier than controlling thought processes and methods?

Mr. WOLF. Yes.

Mr. CONNOLLY. Yes. So different challenge, what we're being asked to do. So you take that—not you, collectively, take that request, come up with something that helps us, because we're worried, your partners in Wassenaar are worried, and you come up with a draft rule. Is that correct?

Mr. WOLF. Correct.

Mr. CONNOLLY. You submit that rule to public comment, including industry comment. Is that correct?

Mr. WOLF. Well, normally, not. Normally with Wassenaar, we rely——

Mr. CONNOLLY. No. No. I was not asking that question. You did?

Mr. WOLF. Oh, yes, absolutely.

Mr. CONNOLLY. I'm just trying to get the sequence.

Mr. WOLF. Okay.

Mr. CONNOLLY. So let me ask the question. Why wouldn't—because you had to pull the rule. So why wouldn't we have reversed that sequence and sought industry's input before we actually issued a draft rule?

Mr. WOLF. At the time of the administration's agreement with the proposed rule, or the control within Wassenaar, our understanding and the understanding of our industry advisory groups was that the scope of the control was quite narrow and only would affect a very small number of products.

So there was no need to do that, or something along those lines. It was only after the fact, as we began to learn more and see how other people read exactly the same words that we had read in 2013, that you can come to other very reasonable conclusions about the broad—the breadth and the scope and the impact of the control.

Mr. CONNOLLY. Right. And to your credit, you pulled them?

Mr. WOLF. Yes.

Mr. CONNOLLY. But I guess I'm a little concerned about the process moving forward, because, okay, this time, we spared ourselves either an embarrassment or a significant, you know, problem. But

I'm—I'm looking at something you said, Ms. McGuire. You were talking about the licensing requirement of the rule. And you said, asking a multinational corporation, who is at risk of a cyber attack, to wait months for a license, to be able to test its network defenses, or to receive the latest protections because security providers are hampered from communicating across borders is downright dangerous.

Do you want to comment on that in terms of the process? Again, I fully commend, you know, the executive branch for seeing an error and pulling it. We don't always do that. Good work. But I'm still worried, though, that maybe the process could have been perfected so that we could have avoided even that. Your comment.

Ms. MCGUIRE. So, thank you for the question. And I think the process piece of this is—is critically important. And while the technical advisory groups within the Department of Commerce were consulted on this issue, no cybersecurity industry was consulted on this issue. There were none that were sitting on the advisory groups, to our knowledge, at the time.

Mr. CONNOLLY. Another problem with the process.

Ms. MCGUIRE. In addition, the advisory committee, our understanding was that the language that was part of the original proposal that the advisory committees saw was not the language that ultimately was adopted at Wassenaar.

So while they may have—they may have said, we don't think there's going to be a lot of problems, what ultimately became enacted was not what was put in front of them.

Mr. CONNOLLY. That's why I suggested—I mean, I've always been a skeptic about export controls, frankly. I mean, maybe good intentions, but we don't live in that kind of world anymore. And trying to actually contain knowledge, very difficult to do.

I know, Mr. Mulholland—are we Irish?

Mr. MULHOLLAND. I am, sir.

Mr. CONNOLLY. God bless him. Let's give him an extra—give him an extra little bit of time here.

Mr. RATCLIFFE. I am Irish, too. You get all the time you want.

Mr. MULHOLLAND. We'll take it.

Mr. CONNOLLY. And let's call it Irish fairness, right?

Mr. MULHOLLAND. I just want to join your point about things. So I used to be in the military, and actually was subject to a predecessor of the Wassenaar inspection and some Russian officers turned up and said, we have a list here that says you have 36 missile launchers. And so we dutifully took them through into our hangars, they pointed to 36, and life was good.

The thing that we're trying to control today is this. And this is actually—Ms. Schneck mentioned partly. This is the code for the Heartbleed security vulnerability. I've blown it up for the sake of illustration, but it's actually 40 lines of code. If I want to proliferate that, I take it around the corner, and I photocopy it, or I email it, or I post it on the Internet. To your point about trying to control knowledge, we're trying to use, and, frankly, in my view, the wrong tool to control this. We're trying to take a physical construct that's worked pretty well for 20-odd years, and we're trying to drop it into the digital world. And, frankly, my view is that that simply does not work.

Mr. CONNOLLY. I couldn't agree with you more.

Mr. Chairman, and I hope the Congress, on a bipartisan basis, will use this and other forums, Mr. Chairman, to explore a radical rethinking of what's in place right now. And it's all well-intentioned, but I just think we're in a new world. And I think we spend a lot of time, and industry is asked to spend a lot of time and money trying to comply with something that is not efficacious any longer.

I thank the chair.

Mr. RATCLIFFE. I thank the gentleman from Virginia for his questions and his comments.

The chair now recognizes the gentleman from North Carolina, Mr. Walker.

Mr. WALKER. Thank you, Mr. Chairman.

I appreciate the panel being out today for an extended witness time, but we do appreciate all of you being here, as well as staff.

Recently completing my first year in the House, it has opened my eyes to the problems that we have specifically in the cybersecurity arena. Also serving on the Department—or the Committee on Homeland Security, as well as the co-chair of the cloud caucus, has really sent me studying this issue and should cause us all great concern.

Congress recently passed the cybersecurity legislation designed to facilitate the efficient and effective sharing of cyber threat data and indicators between the private and the public sectors.

Ms. Schneck, the DHS has a big role to play in that process. The question for you is how would the proposed Bureau of Industry and Security rule, as drafted, impact that sharing?

Ms. SCHNECK. So, thank you for your question. I would defer a lot of the legal around that to my colleagues from Commerce and State, but I'll give you a technical explanation. So the great legislation that you gave us enabled our operation center, the National Cybersecurity and Communications Integration Center, the NCCIC, to be the Center of Threat Indicator Collections with all the best use of private and civil liberties to get it right. But to get the cyber indicators together so that we can create a good contextual picture and push that information out to our, both public and private partners, and enable them to use that information.

This is real time. This is machine to machine. And one of the worries that we're hearing from private sector and others is that this proposed rule would, in some cases, hamper the real-time sharing of information.

Mr. WALKER. Okay. Let me follow-up with you. If you need to defer, that's fine. I don't know, is there a limit on defers before you would have to buy somebody dinner, or drink? I don't know. We'll see. How would the proposed rule impact cybersecurity generally for U.S. companies? Frequent questions wrapped in one. What about critical infrastructure, government agencies? Isn't the rule going to put them at risk at some point?

Ms. SCHNECK. Is that for me?

Mr. WALKER. Yes, it is, unless you need to defer.

Ms. SCHNECK. So our responsibility is to protect all of that, the critical infrastructure, and then the Federal civilian government, and the private industry to include academia, State and local. We

also share among 300—at least 300 other governments' cyber information.

As a scientist, I'll give you an operational discussion. And that is that the best cybersecurity protection we can provide is to understand the most quickly what's happening and make sure that when a cyber actor, this is exactly what an intrusion is, tries to execute their instruction on a machine they don't own, that machine knows, A, not to execute it, or, B, that it's happening so it can tell everybody else about it and not sustain an injury.

Mr. WALKER. Okay.

Ms. SCHNECK. The ability, or the thought that that would get delayed in any of the ways mentioned today is detrimental to our cybersecurity.

Mr. WALKER. Thank you for the——

Mr. Wolf, did you want to add anything to that?

Mr. WOLF. No. But these are exactly points that—I guess, yes. These are exactly the points that were raised in overwhelmingly in the comments, which is why we're here and why we are continuing through the interagency process to try to come up with a solution to address that very concern.

Mr. WALKER. That's fair.

Ms. Goodwin, I believe that technology is a tool I think most of us would agree, tool is a—technology is a tool that could be used for good or bad. In other words, it's not inherently one direction or the other. I think that's a pretty simple concept, but the behavior is.

I'm intrigued by the idea that under Wassenaar, we are choosing to focus on the exporters of software tools instead of looking at the actual users of those tools and how those tools are utilized.

Question for you: Do you think that, perhaps, we should be looking at a cybersecurity regulatory regime that focused on the users?

Ms. GOODWIN. We certainly need to be exploring the questions in a public-private partnership. The challenge of how do you deter criminal behavior? How you deter the bad effects of using surveillance software against those that we're trying to protect here? How do you stop a criminal from committing a criminal act? That's a challenge. But the reality is that 80—81 percent of the security companies in the world are here in the United States.

So regardless of the effect that it's maybe having outside of the United States, it's going to have a larger effect inside the United States. So we have to think about where the right place to regulate is, the use of the software, the intent of the criminal.

Mr. WALKER. Right. And if it is 80 percent, the technology is kind of interfused where it's hard to even separate from one country doing business with the other. And I hope—and I'll yield back with the rest of my time—the international community can influence or encourage this positive, and hopefully beneficial behavior.

Thank you, Mr. Chairman. I yield back.

Mr. RATCLIFFE. I thank the gentleman.

The chair now recognizes the gentleman from Rhode Island, Mr. Langevin.

Mr. LANGEVIN. Thank you, Mr. Chairman. Before I begin my questions, if I could, I would like to submit my original comments to Department of Commerce, the rule and the concerns that I have.

Mr. RATCLIFFE. Without objection.

Mr. LANGEVIN. Thank you, Mr. Chairman.

First of all, I want to, again, thank you, Secretary Wolf, at the Department of Commerce and BIS for bending over backwards to listen to concerns that have been raised here, and in other areas with respect to this rule. You've been very helpful and responsive to those concerns.

Ms. Ganzer and Secretary Van Diepen, I hope it's very clear that you've hit a wall with respect to the way this was negotiated, what was negotiated, and there's pretty broad opposition going forward. So we are hoping that you are going to take that message and go back and get this right, probably by having to renegotiate.

So is that a fair statement? You understand that we have broad opposition here?

Mr. VAN DIEPEN. I certainly understand your statement, Congressman. Again, I think our responsibility is to work hard and find the best solution that both gives us some ability to address the security concerns we're trying to address while avoiding these unintended consequences.

Mr. LANGEVIN. So with respect to criteria for the selection of dual-use items, dual-use goods and technologies to be controlled are those which are major or are key elements for the indigenous development, reduction, use, or enhancement of military capabilities. For selection purposes, the dual-use items should also be evaluated against the following criteria: Bond availability outside participating states; next, ability to control effectively with the export of the goods; next, the ability to make a clear and objective specification of the item; and, last, control by another regime.

So to Ms. Ganzer and Secretary Van Diepen, with respect to clear and objective specification of the items, given the diversity of implementation we've seen in participating States, is the definition clear at the moment?

Furthermore, the director of DARPA has stated that, and I quote, "From a technology perspective, defense and offenses are indistinguishable," of you echoed by the State Department's own defense trade advisory group. Doesn't this preclude objective specification?

Mr. VAN DIEPEN. I don't believe so, Congressman. Everything on the Wassenaar dual-use list, as well as most of the things in category 2, the missile technology and control regime annex, the entire nuclear suppliers' group dual-use list, and the entire Australia group's chemical biological list are dual-use items. These are things that, again, can inherently be used, both for good purposes and bad purposes.

And these have always included not only physical items, but software of various types. So there's a long, experienced, and multilateral export controls of being able to properly specify and properly control dual-use things, including dual-use software. And so, I—again, I think that, you know, our responsibility is to do our best to see if we can appropriately apply that expertise in this instance.

Mr. LANGEVIN. Okay. I would have some concerns with that answer, but let me go next.

With respect to foreign availability, do you believe that intrusion software tools are not available and could not be developed in non-

Wassenaar participating states like Singapore or China, which are home to four of the top 20 engineering and technology universities in the world according to QS rankings?

Mr. VAN DIEPEN. Congressman, I think the genesis of your statement comes from the factors for consideration that Wassenaar uses in judging items. And these are factors for consideration. It's not a checklist that every item must absolutely fulfill each and every one of the things. But we have to look at each of those things and decide whether the benefits or the control outweigh the—the costs or the difficulties of the control.

So, for example, in the Australia group, we're controlling biological pathogens, many of which you can dig out of your own backyard. So there's ubiquitous foreign availability, but it's believed, and we've got a very solid track record, that it's been very advantageous to U.S. security to be able to maintain export controls on those items multilaterally with our partners.

Mr. LANGEVIN. And with respect to ability to effectively control export, do you believe that our regime has the capability to stop transfer of the goods or associated technology given that software can be sent across the globe without passing through a port of entry or other border checkpoint?

Mr. VAN DIEPEN. And, again, for over 25 years, we've controlled, multilaterally, a whole host of different types of software. And even recognizing the inherent challenges of software export controls, it has been felt that we've been able to craft controls where the benefits outweigh the costs. And, again, I would also point to the biological case, where, again, you're talking about individual cells. If you have two of them, they can self-replicate, so it's not all that different from cyber export controls, and yet, again, it has been felt that it has been advantageous for us to have those types of export controls.

Mr. LANGEVIN. Mr. Secretary, my time has expired, but I have to say, I respectfully disagree with each one of your answers. This is a checklist against which we should be—we should be evaluating on the states' value, and I think you've drawn the wrong conclusions. But my time has expired, and I'll yield back.

Mr. RATCLIFFE. I thank the gentleman.

The chair now recognizes the gentleman from Florida, Mr. Clawson.

Mr. CLAWSON. I appreciate y'all coming. I am just going to make one comment, and then I will yield to Congressman Hurd, if that's okay.

First of all, when I looked at the participating countries, I don't see a lot of Asian competitors there. And I know what I would think if I was in private business, y'all. So you were not talking about the obvious. But I had a lot of competition coming from my—from Asia and India, and we can't be playing a different game than them, or we will lose.

So I understand the need to protect the homeland, but there's something obviously wrong with this list if you're going to—if you were trying to influence me to join up, and I saw that list, after my technology had already been stolen a half dozen times, it would be a tough, tough, sell.

Number two, with my facilities around the world, which we have, which I had, customers—you know, customers and facilities all on these lists, the foreign corrupt practice laws and everything, I don't even know how to do this. I wouldn't know how to implement it. It just feels, like, it hits me like a freight train here.

And so—and, look, I spent a lot of time doing this. So, you know, there's got to be—you would have to put it in terms. I spent, you know, yesterday and today trying to think about these things and think to myself and my own business model, how would I do this? And I never really got there. How can I compete, take care of my customers, take care of my competitors, and my suppliers across all these different borders, and not break the law and keep my country safe? So if y'all are going to do that to sitting CEOs, I recommend that you simplify it so we can understand how we get to do all those things at the same time, because I spent a whole life doing it, and I ain't getting there just yet.

I yield back to Mr. Hurd.

Mr. HURD. I thank my colleague from Florida.

This is a lightening round, y'all. We have a lot more questions to get through, and we have to get to votes.

Number one, I always like to start these off by saying something positive. Mr. Wolf, you and the Department of Commerce, great job in recognizing the problems and pulling back the rule. And as you've alluded to, that doesn't happen that often, and that should be commended. And I'm hearing you right, is the technical advisory committees open to—for people to join?

Mr. WOLF. Absolutely. We're always looking for new volunteers.

Mr. HURD. Do you have one on cybersecurity?

Mr. WOLF. We do. We did then, and we have more now.

Mr. HURD. Okay.

Mr. Garfield, are you willing to help populate the committee?

Mr. GARFIELD. Absolutely.

Mr. HURD. Are there other folks on this the panel willing to send someone to that committee?

VOICE. Yes.

Mr. HURD. Mr. Wolf, are you willing to take their input into thinking about what the best next action is?

Mr. WOLF. Absolutely, whether it's as a tact member or just a member of the public, both.

Mr. HURD. What is the best next action? Are you going to leave here, you are going to say, that was a really long hearing, a lot of panelists, Congressman Ratcliffe was very insightful with his questions, and then—and then what happens?

Mr. WOLF. Well, we'll continue discussing among the agencies, bring in not just the usual export control people, but those were expertise——

Mr. HURD. What forum? When is a decision going to be made about whether another proposed rule is going to be done, or you go back to Wassenaar?

Mr. WOLF. Well, anything—everything is on the table, whether to go back to Wassenaar, another proposed rule with edits and clarifications or interpretations or carve out or exceptions.

Mr. HURD. Who makes that decision?

Mr. WOLF. Well, ultimately, it depends upon the consensus of the agencies involved in the process, Commerce, State, and Defense. And then as the one responsible for the rule, I have the final say in terms of signing the rule out. And so the goal, over however many weeks or months we have to work on this, is to see if we can address all of the very legitimate concerns that have been raised today, and then the comments that you all have raised to come up with something that——

Mr. HURD. Copied. Thank you.

Mr. Van Diepen, why do you care more about what the other 31 countries are implementing than the people on this panel and the members of Mr. Garfield's organizations?

Mr. VAN DIEPEN. Respectively, sir, that does not correctly characterize my views. I care very much. I am a United States Government employee. I care about what the United States——

Mr. HURD. What do you think you are going to learn from the other 31 countries that have already implemented this rule?

Mr. VAN DIEPEN. The kinds of issues that have been raised here are generic. They don't uniquely affect the United States. And so to find out how other countries——

Mr. HURD. So how many of those countries that have implemented that rule have the same cybercrime laws that the U.S. has?

Mr. VAN DIEPEN. Unclear, and it's not clear——

Mr. HURD. How many of those countries have the same robust ecology of companies that focus on cybersecurity and practitioners of cybersecurity? I know the answer to this one, by the way, but I want to see if you know.

Mr. VAN DIEPEN. Well, I think, irrespective of the answer to that, all those countries are customers of these people, and information would have to go through——

Mr. HURD. The answer is zero.

Mr. VAN DIEPEN. —and they would have to be licensed——

Mr. HURD. Mr. Van Diepen, the answer is zero. You have a wealth of experience and capabilities here, and they are going to be the ones that tell you how this is going to ultimately be—should be—it's going to be impacted by this industry.

Mr. VAN DIEPEN. Which is exactly why we are consulting with them.

Mr. HURD. We are the ones that are protecting the rest of—the rest of—we have to protect ourselves, and we are protecting the rest of the world's.

Ms. Ganzer, you are in the chair.

Ms. GANZER. Yes.

Mr. HURD. If you were in the chair again in 2013, how would you—how would this have gone differently?

Ms. GANZER. If I had the information I had today, clearly, we would have probably renegotiated this differently. But given the information I had then, I would have made the same decisions.

Mr. HURD. When is the next time you are sitting in the chair? February?

Ms. GANZER. The Wassenaar Arrangement works on an annual cycle where final decisions are not made until December, but proposals are due in—in March and are debated throughout the year.

Mr. HURD. Have you done an industry guidance on this forensics rule that has been brought up? Is there not a rule on forensics?

Ms. GANZER. We don't have one under discussion right now. I'm not aware of one. If we agree to one that we are working to implement, I would have to—I would have to take that question back. I don't know, sir.

Mr. HURD. Mr. Wolf?

Mr. WOLF. Well, the topic is of general discussion, but there isn't anything specific on the table to be able to respond to, no.

Mr. HURD. So the general topic of forensics, forensics tools, for use on understanding a person's network is going to be up for general discussion at Wassenaar at the next conversation?

Mr. WOLF. Perhaps. I don't know what some other country might bring up, but it's not something that we have right now under discussion.

Mr. HURD. If this does come up, I would suggest you reach out to industry first and before you have to figure out what your left and right bound is for negotiation.

I yield back the time that I do not have.

Thank you very much, Mr. Chairman.

Mr. RATCLIFFE. I thank the gentleman.

The chair recognizes my friend and colleague from Texas, Sheila Jackson Lee.

Ms. JACKSON LEE. Thank you so very much. We have a vote on the floor of the House, but I indicated that this was so important and provocative, I'm going to try to be as quickly as I can. And be as successful as the on-site kick was last evening.

But let me try to get to the government. Mr. Wolf and our two distinguished State Department representatives, you have had a series of questions by members. Can I get a yes-or-no answer that you are going back to the drawing board. We know that there is an agreement that's going to be coming forward, suggestions and ideas, to give us an opportunity to go back to this issue again, Ms. Ganzer. But am I sensing that you understand that there needs to be a regulatory revisit on these issues?

Mr. Wolf, yes or no, please?

Mr. WOLF. Yes.

Ms. JACKSON LEE. Ms. Ganzer?

Ms. GANZER. Absolutely.

Ms. JACKSON LEE. Mr. Van Diepen?

Mr. VAN DIEPEN. On the rule, yes, ma'am.

Ms. JACKSON LEE. All right. Let me—and we have opportunities for the agreement itself coming—going forward. But let me—let me try to pointedly get back to our experts here and say, this reminds me of the DMCA, which Congress did pass, but negatively impacted encryption research. And interestingly enough, all of us are talking about encryption now.

So I want to get to the point of saying where we are in terms of impacting you and the new partnerships. The President just had meetings with those in Silicon Valley. We know that we are intertwined together.

May I start with Mr. Garfield to find out from you how much this will impact negatively research, and getting to the solutions of

what we are interested in as you represent your vast number of participants?

Mr. Garfield?

Mr. GARFIELD. I'll be brief. It will impact significantly. And part of the frustration with the current course of the discussions is rather than recognizing that the issue at play here is not just the regulation of software, but the need for real-time reaction in response to cybersecurity, we're thinking about this as simply something we have faced before.

That's why we need to think beyond the box of export control and really start over.

Ms. JACKSON LEE. Well, and I don't necessarily like it for starting over, but I like it for the forthright way that you're saying that we have an issue that needs serious attention.

Let me just go quickly to Ms. Goodwin and Mr. Mulholland. And, Mr. Mulholland, I think it was you that said, all options are on the table. I have introduced H.R. 85, Terrorism Prevention and Critical Infrastructure and Protection Act, which deals with identifying threats, isolating damaging activities, but really, wants to work with industry on these elements. But if I can just get you to answer the question. As I said, I'm speaking fast only because my colleagues are here and we are voting. But to get to the point of what the impact would be if we do not fix it. And Mr. Mulholland as well, and I think we have Ms. McGuire there as well. And let me thank Dr. Schneck very much for the work she's done with us in Homeland Security.

Ms. Goodwin.

Ms. GOODWIN. Ms. Jackson Lee, we get over 1,000 vulnerability reports that come into Microsoft every year, and those need to be triaged. We need to work them with the finders from around the world and with our teams internally, and those internal teams sit all around the world. So we can be looking at 1,000 vulnerabilities times three, four, five export licenses just to triage vulnerabilities. That's not talking malware; that's not talking about new tools or new issues. That's just to be able to do our daily work.

And so that would, from what we understand, eclipse the total volume of licenses that the Department of Commerce grants.

Ms. JACKSON LEE. That would not work.

Mr. Mulholland.

Mr. MULHOLLAND. So I will echo the points that Ms. Goodwin made. We have a similar situation. But let me take a different angle. Security research is not going to stop. There are—Siri told me there are 206 countries in the world. There's 41 in Wassenaar. My math tells me that's 165 countries that are not in Wassenaar, perhaps two-thirds of software developers in the world. Software security research will continue, but it will happen in three different ways.

Mr. MULHOLLAND. Either security researchers will finally just give up, it's just too hard. That's not good for us. They will publish the information on the Internet because there is a carve-out, from my understanding, that if the information is made public on the Internet, effectively open-sourced, then it does not require a license. That doesn't help me because the bad guys have just found out about the issue at the same time I have. That's not good for

us. It's not good for U.S. companies. Or the third one, which, frankly, 20 years of working in this industry and the cynicism that can develop with that, these exploits will, frankly, end up on the black market. And there will be cottage industries developing in some of the countries that have been mentioned that will spring up. And these oppressive regimes, the only impact that they will find is that they will have to spend more money because they will be going to the highest bidder——

Ms. JACKSON LEE. Thank you. I want to get Ms. McGuire. And I'm going to let Dr. Schneck, Ms. Schneck, just finish, that Homeland Security is committed to working, too. Ms. McGuire, in this brief moment.

Ms. MCGUIRE. I will just echo that the rule as proposed here in the United States will not do anything to deter the availability of these tools. And I will just finish by saying at the end of the day, the underlying language in the Wassenaar Arrangement on cybersecurity is flawed and must be renegotiated.

Ms. JACKSON LEE. Thank you. Ms. Schneck, Homeland Security——

Ms. SCHNECK. Bottom line, we have to, together as interagency, with all of our industry partners and any input we can possibly get absolutely revisit this proposed rule.

Ms. JACKSON LEE. Let me thank the chairman and Ms. Kelly so very much for your kindness. And may I ask unanimous consent, Mr. Chairman, thank the witnesses, to submit into the record from the Internet Association a letter dated January 12, 2016.

Mr. RATCLIFFE. Without objection.

Ms. JACKSON LEE. Thank you so very much, Mr. Chairman.

Mr. RATCLIFFE. I thank the witnesses for their testimony. I can pretty much assure you that at least some members will have some additional questions for the witnesses. And we will ask you to respond to those in writing. The hearing record will be open for 10 days. Without objection, the subcommittees stand adjourned. Thank you.

[Whereupon, at 4:27 p.m., the subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

WASHINGTON OFFICE:
2160 Rayburn House Office Building
Washington, DC 20515
(202) 225-3816

DISTRICT OFFICE:
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRES HOME OFFICE:
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEIGHTS OFFICE:
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 961-4070

FIFTH WARD OFFICE:
4300 LYONS AVENUE, SUITE 200
HOUSTON, TX 77020
(713) 227-7740

Congress of the United States
House of Representatives
Washington, DC 20515

COMMITTEES:
JUDICIARY
SUBCOMMITTEES:
COURTS, INTELLECTUAL PROPERTY AND THE INTERNET
IMMIGRATION AND BORDER SECURITY

HOMELAND SECURITY
SUBCOMMITTEES
RANKING MEMBER
BORDER AND MARITIME SECURITY
TRANSPORTATION SECURITY

SENIOR WHIP
DEMOCRATIC CAUCUS

CONGRESSWOMAN JACKSON LEE

STATEMENT FOR A

JOINT HEARING

COMMITTEE ON HOMELAND SECURITY'S SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES AND COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM'S SUBCOMMITTEE ON INFORMATION TECHNOLOGY

Entitled the, "Wassenaar: Cybersecurity & Export Control"

Tuesday, January 12, 2016

- Chairman McCaul and Ranking Member Thompson of the Committee on Homeland Security, Chairman Ratcliff and Ranking Member Richmond of the Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies thank you for the opportunity to hold a joint hearing with the Committee on Oversight and Government Reform's Subcommittee on Information Technology on the topic of the Wassenaar: Cybersecurity & Export Control ruling making currently underway.

- I thank today's witnesses for testifying before the joint hearing, which includes:

- Ms. Ann K. Ganzer, Director of Conventional Arms Threat Reduction, with the Bureau of International Security and Nonproliferation for the U.S. Department of State;
- The Honorable Kevin J. Wolf, the Assistant Secretary for Export Administration for the U.S. Department of Commerce;
- Ms. Phyllis Schneck, the Deputy Under Secretary for Cybersecurity and Communications for the National Protection and Programs Directorate U.S. Department of Homeland Security;
- Ms. Cheri Flynn McGuire, the Vice President of Global Government Affairs and Cybersecurity Policy with Symantec;
- Mr. Iain Mulholland, the Vice President of Engineering Trust and Assurance with VMware, Inc.;
- Ms. Cristin Flynn Goodwin, the Assistant General Counsel for Cybersecurity with the Microsoft Corporation; and
- Mr. Dean C. Garfield, the President and CEO, of the Information Technology Industry Council.

- The hearing will give the committees an opportunity to learn more about the federal agencies responsible for policy development and enforcement of sensitive dual-use cybersecurity technology export controls, and to hear from private sector stakeholders regarding the ramifications of newly added cybersecurity export controls and definitions contained in the Wassenaar Arrangement.

- The Wassenaar Arrangement was established to contribute to regional and international security and stability, by promoting transparency and greater responsibility in transfers of conventional arms, dual-use goods and technologies.

- Wassenaar Agreement involves 41 participating nations who seek, through their national policies, to ensure that transfers of these items do not contribute to the development or enhancement of military capabilities which undermine these goals, and are not diverted to support such capabilities.

- The goal of the Wassenaar Agreement is to regulate the export of guns, other conventional weapons, and their components (such as fissile material).

- As a member of the group of nations that abide by the Wassenaar Agreement the United States agreed to prepare the rule that would govern cyber surveillance technology under the Wassenaar Agreement.

- In December 2013, the list of controlled technologies covered under the Wassenaar Agreement was amended to include cyber surveillance systems for the first time, in response to reports linking exports of Western surveillance technologies to human rights abuses in countries such as Bahrain and United Arab Emirates, Turkmenistan, and Libya.

- The Department of Commerce's Bureau of Industry and Security (BIS) is in the process of preparing to issue a proposed rule that reflects 2013 cyber additions to the

Wassenaar Arrangement, pertaining to export controls of dual-use 'intrusion software', commonly known as cyber and information security software.

- In May 2015, the BIS published its proposed implementation of changes to the arrangement and received an overwhelming amount of comments opposed to the proposed rule, including widespread opposition by industry and the academic and research community.

- The U.S. academic and research communities had serious concerns regarding enforcement of the conditions that may be imposed base upon a new Wassenaar Rule for Cyber surveillance technology: such as the proposed rule is too broad for the established objectives under the narrow definition which states that the rule is not to apply to software or technology that is generally available to the public or used as part of basic scientific research.

- The chief opposition to the BIS proposed rule is that it does not include the exceptions language in the guidance provided by the Wassenaar cyber surveillance guidelines that should have informed the BIS rulemaking process and it goes much further than the Wassenaar text on cyber surveillance.

- The BIS rule would without exception cover systems, equipment, components and software specially designed for the generation, operation or delivery of, or communication with, intrusion software include network penetration testing products that use intrusion software to identify vulnerabilities of computer and network-capable devices.

- Confusion was created by the BIS proposed rule because it appeared to many, perhaps in error, that the rule prohibited the sharing of vulnerability research without a license.

- Computer scientist and computer security research note often the unintended adverse impact of the Federal government's efforts in passage of the Digital Millennium Copyright Act (DMCA) which negatively impacted encryption research in the United States when private sector companies were allowed to file civil suits against academic computer security researchers.

- The DMCA is cited by computer security academic researchers as the single most damaging law to impede the development of strong encryption consumer products and their work to solve encryption problems which emerge as the science advanced globally.

- Improving computing security by providing strong cyber security products to protect computer networks is essential to protecting our financial institutions; critical infrastructure; and consumer privacy.

- The goal of regulating cybersecurity products that are intended to aid repressive regimes in monitoring citizens and violating human rights is something that we should all be able to support.

- The Wassenaar Rule should be careful to promote the positive intent of the stated purpose without impeding the

important role of cybersecurity in protecting computer networks.

- The BIS received a tremendous number of comments, which under law they must consider in the development of a rule that would have the force of law.

- It is my hope that they will work closely with industry and the academic research community to ensure that the rule conforms the purpose and intent of the Wassenaar Agreement on cyber surveillance technology.

- I look forward today's witnesses' testimony.

- I yield back.

- Thank you.

Congress of the United States
Washington, DC 20515

December 16, 2015

The Honorable Susan E. Rice
Assistant to the President for National Security Affairs
The White House
1600 Pennsylvania Ave NW
Washington, DC 20500

Dear Ambassador Rice:

The Department of Commerce is preparing to issue a proposed rule that has the potential to significantly undermine the United States' cybersecurity posture. We write to share our concern that this rulemaking, which is part of an effort to implement the 2013 additions to the Wassenaar Arrangement pertaining to export controls of "intrusion software," could seriously hinder our national security without a significant overhaul.

The original proposed rule, issued by the Bureau of Industry and Security (BIS), contained flaws that some of us highlighted during the public comment period. The definition of intrusion software, agreed upon by the Department of State at the Wassenaar Plenary, is very broad to the point that it includes a number of products regularly used for cybersecurity research and defense. The definition is so all-encompassing that any implementation must greatly narrow the range of affected technologies; if that proves unfeasible, the language of the Arrangement itself may need to be renegotiated. BIS was cognizant of this challenge when drafting the initial rule; unfortunately, the proposed solution – attempting to draw a line between offensive and defensive cyber tools – was misguided, as defenders need access to exploits to test their networks. This artificial distinction, combined with the lack of a waiver of deemed export rules, could have a chilling effect on research, slowing the discovery and disclosure of vulnerabilities and impeding our nation's cybersecurity. These concerns were echoed by nearly three hundred public comments representing a diverse array of interests. Consequently, after evaluating these comments, we are concerned that BIS may lack the policy expertise to appropriately weigh these critically important security interests.

We agree that the export of sophisticated hacking technologies to criminal organizations or repressive regimes is a legitimate national security concern. However, it is vitally important that the rule created to improve national security – by preventing these software exports – does not itself impair security efforts and we strongly believe the initial rule, as proposed by BIS, would have done just that.

As you know, governmental and private sector networks are under near constant attack from sophisticated adversaries using cutting-edge technologies. To defend against these threats, network operators need real-time access to the best available cybersecurity technologies. The proposed BIS rule would have dramatically reduced our ability to defend our nation's networks – hindering companies' abilities to acquire and utilize new security technologies as well as

PRINTED ON RECYCLED PAPER

impeding vulnerability disclosure and information sharing – while only marginally reducing malicious actors' abilities to use hacking tools.

Throughout the rulemaking process, BIS has been very accommodating to stakeholders, participating in numerous listening sessions and working closely with its Technical Advisory Committees. We believe that clear advice from the Executive Office of the President will help BIS and State put these comments into context. Therefore, we request that you take an active role in collaborating with BIS and State to reevaluate the 2013 Wassenaar additions. Your guidance will help them conform to the United States' broader cybersecurity strategy and holistically evaluate the net effects on national security. Furthermore, your involvement will help resolve the uncertainty facing businesses as they await resolution of what has already been an overlong process.

We thank you for your leadership on this issue, and we look forward to working with you to support our nation's cybersecurity.

Sincerely,

JAMES R. LANGEVIN
Member of Congress

MICHAEL T. MCCAUL
Member of Congress

BENNIE THOMPSON
Member of Congress

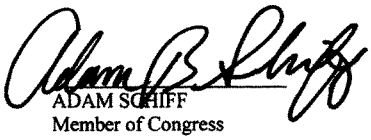
FRED UPTON
Member of Congress

JOHN CONYERS, JR.
Member of Congress

BOB GOODLATTE
Member of Congress

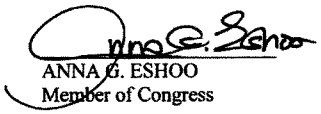
ADAM SMITH
Member of Congress

MAC THORNBERRY
Member of Congress



ADAM SCHIFF
Member of Congress

JASON CHAFFETZ
Member of Congress



ANNA G. ESHOO
Member of Congress

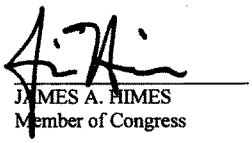
LAMAR SMITH
Member of Congress

TED W. LIEU
Member of Congress

PETE SESSIONS
Member of Congress

ZOE LOFGREN
Member of Congress

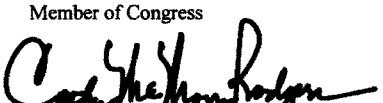
STEVE CHABOT
Member of Congress



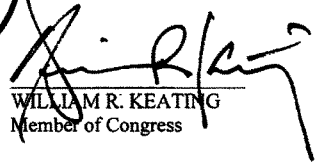
JAMES A. HIMES
Member of Congress

CANDICE S. MILLER
Member of Congress

JAN SCHAKOWSKY
Member of Congress

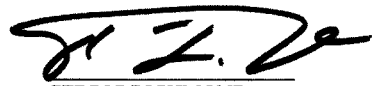


CATHY MCMORRIS RODGERS
Member of Congress



WILLIAM R. KEATING
Member of Congress

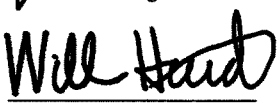
BILL FLORES
Member of Congress



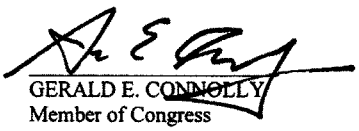
CEDRIC RICHMOND
Member of Congress

JOHN RATCLIFFE
Member of Congress

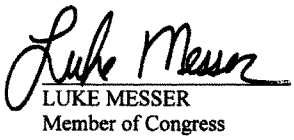
ROBIN KELLY
Member of Congress



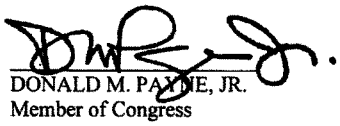
WILL HURD
Member of Congress



GERALD E. CONNOLLY
Member of Congress



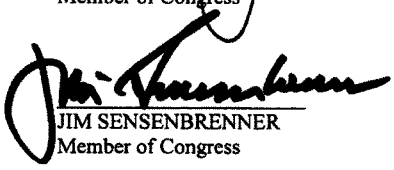
LUKE MESSER
Member of Congress



DONALD M. PAYNE, JR.
Member of Congress

MIKE KELLY
Member of Congress

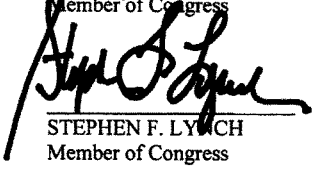
DEREK KILMER
Member of Congress



JIM SENSENBRENNER
Member of Congress

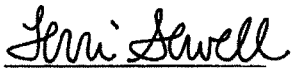
SUZAN DELBENE
Member of Congress

BILL JOHNSON
Member of Congress



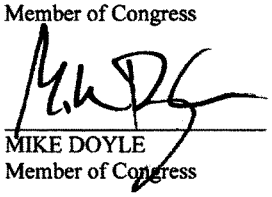
STEPHEN F. LYNCH
Member of Congress

LEONARD LANCE
Member of Congress



TERRI SEWELL
Member of Congress

DANIEL M. DONOVAN, JR.
Member of Congress

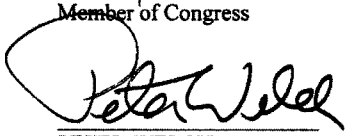


MIKE DOYLE
Member of Congress

DOUG COLLINS
Member of Congress

TONY CARDENAS
Member of Congress

DAVE TROTT
Member of Congress

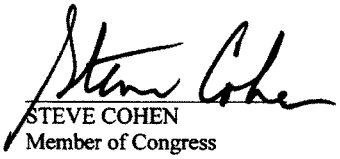


PETER WELCH
Member of Congress

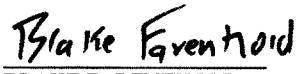
KEN BUCK
Member of Congress

HAKEEM JEFFRIES
Member of Congress

MIMI WALTERS
Member of Congress

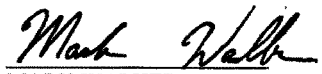


STEVE COHEN
Member of Congress



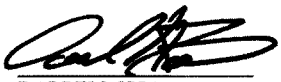
BLAKE FARENTHOLD
Member of Congress

DORIS MATSUI
Member of Congress



MARK WALKER
Member of Congress

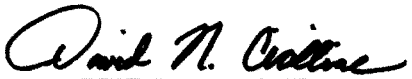
SCOTT PETERS
Member of Congress



DARRELL ISSA
Member of Congress

BRENDA L. LAWRENCE
Member of Congress

MIKE BISHOP
Member of Congress



DAVID N. CICILLINE
Member of Congress

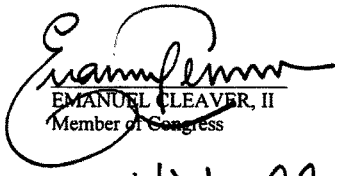
ROBERT PITTENGER
Member of Congress

DONALD S. BEYER, JR.
Member of Congress

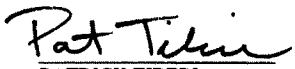
TRENT FRANKS
Member of Congress

ERIC SWALWELL
Member of Congress

TOM MARINO
Member of Congress



EMANUEL CLEAVER, II
Member of Congress

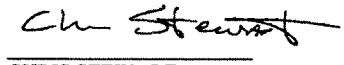


PATRICK TIBERI
Member of Congress

BONNIE WATSON COLEMAN
Member of Congress

BARBARA COMSTOCK
Member of Congress

MICHAEL M. HONDA
Member of Congress

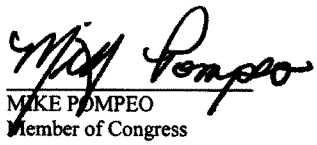


CHRIS STEWART
Member of Congress

BILL FOSTER
Member of Congress

DAVID ROUZER
Member of Congress

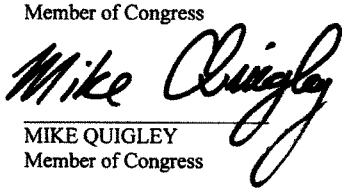
RON KIND
Member of Congress



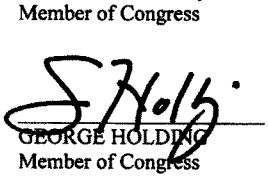
MIKE POMPEO
Member of Congress

C. A. 'DUTCH' RUPPERSBERGER
Member of Congress

CHARLES BOUSTANY, JR., MD
Member of Congress

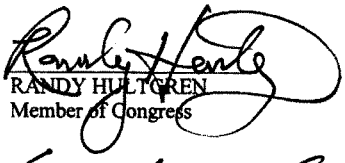


MIKE QUIGLEY
Member of Congress

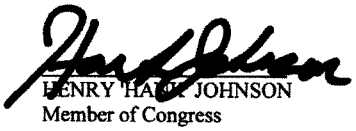


GEORGE HOLDING
Member of Congress

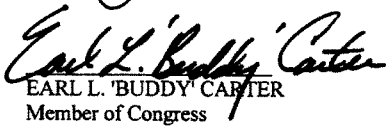
EARL BLUMENAUER
Member of Congress



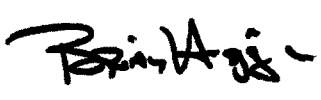
RANDY HULTGREN
Member of Congress



HENRY 'HANK' JOHNSON
Member of Congress



EARL L. 'BUDDY' CARTER
Member of Congress

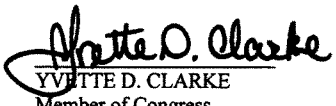


BRIAN HIGGINS
Member of Congress

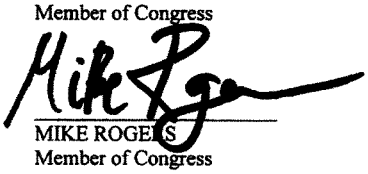
CHRIS COLLINS
Member of Congress

JUDY CHU
Member of Congress

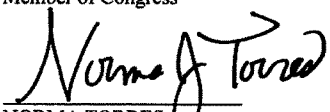
JOE WILSON
Member of Congress



YVETTE D. CLARKE
Member of Congress



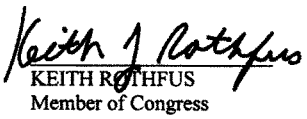
MIKE ROGERS
Member of Congress



NORMA TORRES
Member of Congress

PETER KING
Member of Congress

JACKIE SPEIER
Member of Congress



KEITH ROTHFUS
Member of Congress

KAREN BASS
Member of Congress

BARRY LOUDERMILK
Member of Congress

KATHLEEN M. RICE
Member of Congress

PATRICK MEEHAN
Member of Congress

TAMMY DUCKWORTH
Member of Congress

MARSHA BLACKBURN
Member of Congress

G.K. BUTTERFIELD
Member of Congress

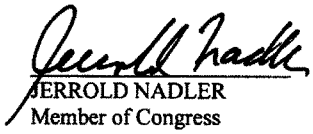
DAVID P. JOYCE
Member of Congress

JOE COURTNEY
Member of Congress

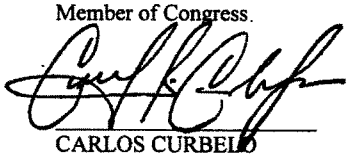
ANN WAGNER
Member of Congress

RICK LARSEN
Member of Congress

JOHN KATKO
Member of Congress

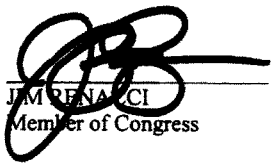


JERROLD NADLER
Member of Congress



CARLOS CURBELO
Member of Congress

TED DEUTCH
Member of Congress



JIM RENACCI
Member of Congress

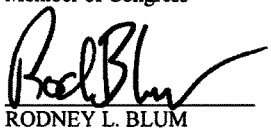
PATRICK MURPHY
Member of Congress

KENNY MARCHANT
Member of Congress

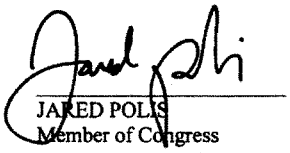
GREGORY W. MEEKS
Member of Congress

DAVID SCHWEIKERT
Member of Congress

BEN RAY LUJAN
Member of Congress



RODNEY L. BLUM
Member of Congress



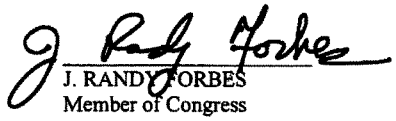
JARED POLIS
Member of Congress

DANA ROHRABACHER
Member of Congress

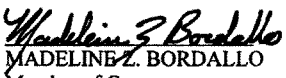
ALCEE HASTINGS
Member of Congress

LYNN JENKINS
Member of Congress

ALBIO SIRES
Member of Congress



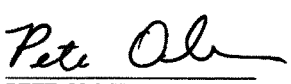
J. RANDY FORBES
Member of Congress



MADELINE Z. BORDALLO
Member of Congress

GREG WALDEN
Member of Congress

JOE BARTON
Member of Congress



PETE OLSON
Member of Congress

GUS BILIRAKIS
Member of Congress

SAM GRAVES
Member of Congress

JOHN SHIMKUS
Member of Congress

SUSAN W. BROOKS
Member of Congress

FRANK A. LOBIONDO
Member of Congress

July 20, 2015

Catherine Wheeler
Director, Information Technology Control Division
c/o Regulatory Policy Division
Bureau of Industry and Security
Room 2099B, US Department of Commerce
14th St and Pennsylvania Ave NW
Washington, DC 20230

Re: RIN 0694–AG49 – Wassenaar Arrangement 2013 Plenary Agreements Implementation: Intrusion and Surveillance Items

Dear Director Wheeler:

Thank you for the opportunity to comment on the Bureau of Industry and Security's proposed rulemaking RIN 0694–AG49, regarding the addition of new dual-use technologies to the Wassenaar Arrangement Annex. We write as Members of Congress with an abiding interest in national security in general and cybersecurity in particular. While we are sympathetic to BIS's goals in implementing the 2013 additions, we are deeply concerned that the regulations could unintentionally weaken our security posture.

There is no doubt that, in the wrong hands, offensive hacking tools can cause great damage. Whether it results in the exfiltration of sensitive data, as in the recent breach of the Office of Personnel Management, or the execution of malicious commands, such as those that destroyed thousands of computers at Sony Pictures Entertainment, malware has proved to be a great scourge of our digital age.

As such, there are very legitimate concerns that intrusion software developed in countries party to Wassenaar could find its way into the hands of criminal organizations or even repressive regimes. In fact, the recent dump of data from Hacking Team, an Italian security firm, bears out these fears. Leaked emails and spreadsheets strongly suggest that Hacking Team sold tools to the Ethopian government that were later used to commandeer journalists' computers so that they could be monitored. Worse, Hacking Team files indicate that the company sold its products to the government of Sudan, a country that is sanctioned by most of the international community due to its history of violence against its people.

When the Wassenaar Arrangement Plenary agreed to add intrusion software to the annex, it was exactly technologies like Hacking Team's that the members intended to regulate. Unfortunately, the agreed upon definition for intrusion software is quite broad, embracing a number of products that are solely intended for research. BIS's proposed implementation of the new definitions, while cognizant of this potential problem, serves only to exacerbate it by drawing a misguided line between offensive and defensive cyber tools. Combined with the lack of a waiver of deemed export rules, this could have a chilling effect on research, slowing the disclosure of vulnerabilities and impairing our nation's cybersecurity.

Zero-Day Vulnerabilities

Of paramount concern in the proposed rule is BIS's treatment of zero-day or rootkit capabilities within intrusion software. BIS does not define "zero-day" or "rootkit" in the NPR, which is, in itself, troubling. Our interpretation of the rule views a "zero-day" as a software vulnerability that does not yet have a patch

designed to mitigate it. We understand a "rootkit" to be intrusion software with the capability of giving its user unfettered – root – access to the underlying operating system. BIS indicates that license requests for software making use of such capabilities would be presumptively denied.

We understand that BIS's intent in including these additional terms was to delineate between offensive and defensive intrusion software. Because there are no patches for zero-days, a firm doing a penetration test to judge a client's patch management program would have no need to include a zero-day in its testing suite. However, cybersecurity risk management frameworks operate on the assumption that breaches will happen, and that a manager must therefore not rely solely on perimeter defenses. Network operators, therefore, may wish to assess how their systems respond to a wholly novel threat. Preventing the export of testing frameworks that make use of zero-days could, therefore prevent comprehensive evaluation of cybersecurity posture.

Rootkits pose a similar problem. Demonstrating a vulnerability or performing a penetration test does not always require the vulnerability to acquire root access. However, certain vulnerabilities, particularly those targeted at the operating system, are based on privilege escalation – gaining administrator access without appropriate credentials – and any related demonstration code would necessarily be considered a rootkit. Furthermore, mature cybersecurity strategies should recognize the potential for rootkit infection and employ detection measures that rely on alternate means, such as traffic analysis, to identify compromised systems. Precluding export of rootkits can thus also impact cybersecurity.

Deemed Export

We are also troubled by the implications of applying the "deemed export" regime to intrusion software, a rule that has not been adopted by European Union members in implementing the Wassenaar Arrangement. Many American companies have multinational footprints, and even those solely operating within the United States often employ foreign nationals, particularly in fields like cybersecurity that suffer from an acute talent deficit. Similarly, academic institutions around the country have a significant minority of foreign graduate students, many of whom are at the front lines of information security research.

We see two significant challenges in applying the deemed export rules to these technologies. Third parties often disclose vulnerabilities to anonymous email addresses established specifically for this purpose. A security researcher thus has no way of knowing who precisely will see the disclosure. Requiring a careful chain of custody for researchers to ensure they don't inadvertently "export" a vulnerability by sharing it with foreign national employed by a developer could easily disrupt the entire reporting ecosystem.

Furthermore, if companies or researchers are required to segregate data based on nationality or to apply for a license to share information with their own students or employees, research will suffer. Companies may be unable to share threat data with their own international affiliates, at least not in a timely manner. Because hackers can attack overseas just as easily as domestically, any weak system with access to a business's internal network represents a serious vulnerability.

As you are no doubt aware, Congress is very interested in expanding information sharing of cyber threat indicators. Two bills have already passed the House this session attempting to incentivize information sharing, and the Senate Select Committee on Intelligence has favorably reported a similar measure. We hope that the final BIS rule will further these efforts, or at the very least not hinder them.

Research Exemption

In its conversations with stakeholders, BIS has emphasized that publicly available intrusion software is not subject to export controls. Beyond the Constitutional requirements that may motivate it, this is a wise

policy that helps foment an innovative research environment. However, we are concerned that BIS is overly reliant on the public research exemption as a way for intrusion software developers to escape otherwise broad regulations.

Responsible disclosure first involves a researcher privately contacting the owner of a piece of vulnerable software. Sometimes, the vulnerability in question will be made public because the developer refuses to patch it. Sometimes, the vulnerability will be patched, and then the exploit will be incorporated into open source penetration testing software. However, there are cases when an exploit will be patched silently in an effort to avoid giving malicious actors a blueprint to flaws in a system. The BIS rule, as proposed, also does not clarify exactly when an exploit goes from being controlled to being public, which could further complicate the efforts of security researchers.

Conclusion

Part of the difficulty faced by BIS stems from the underlying language agreed upon by the Wassenaar parties. That "intrusion software" encompasses vulnerabilities at all is something that the international community may wish to revisit during future negotiations. Information systems security is still a new field, and policy tools are still being developed and calibrated.

The recent Hacking Team revelations have driven home the need for reasonable export controls on software that can be used by criminals and governments to attack citizens around the globe. While we have serious concerns about some of the provisions of the proposed rule, we do not doubt the need for it. To ensure that the rule is narrowly targeted, we strongly encourage BIS to consider issuing another draft rule for comment before finalizing the implementation.

Thank you again for the opportunity to comment on this important issue. We must also commend BIS for its extensive outreach effort – both through the Department of Commerce and the Department of Homeland Security – with stakeholders in academia and industry. If you have any questions regarding the submittal, please contact the Office of Congressman Langevin at (202) 225-2735.

Sincerely,

JAMES R. LANGEVIN
Member of Congress

DAVID SCHWEIKERT
Member of Congress

MICHAEL MCCAUL
Member of Congress

TED LIEU
Member of Congress

Internet Association

January 12, 2016

The Honorable Will Hurd
Chairman, Subcommittee on Information Technology
Committee on Oversight and Government Reform
U.S. House of Representatives
2157 Rayburn House Office Building
Washington, D.C. 20515

The Honorable John Ratcliffe
Chairman, Subcommittee on Cybersecurity Infrastructure Protection, and Security Technologies
House Committee on Homeland Security
H2-176 Ford House Office Building
Washington, D.C. 20515

The Honorable Robin Kelly
Ranking Member, Subcommittee on Information Technology
Committee on Oversight and Government Reform
U.S. House of Representatives
2471 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Cedric Richmond
Ranking Member, Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies
House Committee on Homeland Security
H2-117 Ford House Office Building
Washington, D.C. 20515

Dear Chairman Hurd, Chairman Ratcliffe, Ranking Member Kelly, and Ranking Member Richmond:

The Internet Association respectfully requests that this letter be submitted to the record for today's hearing entitled "Wassenaar: Cybersecurity and Export Controls."

The Internet Association is the unified voice of the Internet economy, representing the interests of leading Internet companies and their global community of users.[1] We are dedicated to advancing public policy solutions to strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. Network security is of paramount importance to our member companies and their end users. They work tirelessly to defend their networks and their users' data from unlawful intrusions. Private companies frequently share information about emerging threats through commercial platforms, email lists, conferences, forums, and open platforms such as ThreatExchange hosted by Facebook, which is used by companies including Coinbase, Etsy, Google, LinkedIn, Netflix, Pinterest, Salesforce, Twitter, Yahoo, and Yelp. Public policies that undermine the ability of security researchers to protect networks – whether by design or by default – are therefore highly relevant and important to us.

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies is a multilateral agreement that has published lists since 1996 to ensure responsibility and transparency in global arms trade through control of certain goods, software, and information technologies for export by the 41 participating states, including the United States. The Wassenaar

[1] The Internet Association's members include Airbnb, Amazon, auction.com, Coinbase, Dropbox, eBay, Etsy, Expedia, Facebook, FanDuel, Gilt, Google, Groupon, Handy, Intuit, LinkedIn, Lyft, Monster Worldwide, Netflix, Pandora, PayPal, Practice Fusion, Rackspace, reddit, Salesforce.com, Snapchat, SurveyMonkey, TripAdvisor, Twitter, Yahoo, Yelp, Uber, Zenefits, and Zynga.

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org

Agreement was amended to include controls for certain "intrusion software" under the 2013 Plenary Agreements Implementation on Intrusion and Surveillance Items. The Internet Association appreciates the intent of the 2013 changes to target illegal surveillance and exfiltration of data from a target without authorization; however, without narrow construction, controls on intrusion software could have inverse effects of compromising network security research and increasing the risk of network vulnerabilities.

On May 20, 2015, after a number of conversations with leaders in industry, the Bureau of Industry and Security (BIS) issued a proposed rulemaking to implement the 2013 changes regarding intrusion software. Unfortunately, this flawed rulemaking includes broad definitions and wide reaching export controls that would impede our ability to defend our networks' from attackers. The Internet Association filed public comments to the BIS proposal and has attached a copy to this letter. BIS has worked with stakeholders to capture their concerns. However, the current draft rule still raises significant issues and challenges for security research.

To ensure that the rulemaking would target illegal surveillance and exfiltration of data from a target without authorization as intended, the Internet Association urges the following changes, as submitted to the BIS in response to their request for comments in July 2015:

1. Introducing an intra-company exception;

2. Focusing on exfiltration and the use of cybersecurity items for unauthorized activities, not the items' technical capabilities;

3. Maximizing clarity around acceptable uses that do not require a license;

4. Including more detailed language in the regulations' text and preamble, similar to was has been included in the BIS FAQs;

5. Sharpening the definition of "Intrusion Detection Systems" to include technologies that are both system and network-based, in order to avoid conflating network intrusion detection systems (NIDS)/man-in-the-middle (MITM) tools with surveillance tools; and

6. Providing better and more comprehensive guidance to help individuals and organizations understand their obligations under the proposed rules.

As the efforts to implement the 2013 changes to the Wassenaar Agreement regarding intrusion software have continued, Congress has recognized that such changes could have a detrimental effect on national security. Most recently, 126 bipartisan Members of the House of Representatives signed a letter requesting that the Administration reevaluate the 2013 Wassenaar changes in light of the security concerns and uncertainty facing businesses.[2] The Internet Association commends the work done by Members, including many on these Committees, to urge the Administration to avoid implementation measures that would hinder national security by restricting critical security research.

[2] Letter from 126 Members of U.S. House of Representatives to The Honorable Susan Rice, Assistant to the President for National Security Affairs (December 16, 2015).

Internet Association

We thank you for your attention to this important matter, and urge your Committee to work with the Administration to improve the proposed rules to be minimal and narrowly targeted.

Respectfully Submitted,

Michael Beckerman
President & CEO

CC: The Honorable Jason Chaffetz, Chairman of the House Committee on Oversight and Government Reform
The Honorable Michael McCaul, Chairman of the House Committee on Homeland Security
The Honorable Elijah Cummings, Ranking Member of the House Committee on Oversight and Government Reform
The Honorable Bennie Thompson, Ranking Member of the House Committee on Homeland Security

1333 H Street NW, Washington, DC 20005
12th Floor, West
www.InternetAssociation.org