RPTR MAAR

EDTR ROSEN

# 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, Gosar, Kelly,

Connolly, Duckworth, and Lieu.

Present for Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies: Representatives Ratcliffe, King, 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 Communication 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 proposed 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.

[Prepared statement of Mr. Langevin follows:]

******** COMMITTEE INSERT ********

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 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 White House'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 control 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 convention 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 export control regime, where 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.

STATEMENTS OF VANN H. VAN DIEPEN, PRINCIPAL DEPUTY ASSISTANT SECRETARY FOR INTERNATIONAL SECURITY AND NONPROLIFERATION, DEPARTMENT OF STATE; HON. KEVIN J. WOLF, ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE; ANN K. GANZER, DIRECTOR OF CONVENTIONAL ARMS, THREAT REDUCTION, BUREAU OF INTERNATIONAL SECURITY AND NONPROLIFERATION, DEPARTMENT OF STATE; PHYLLIS SCHNECK, DEPUTY UNDER SECRETARY FOR CYBERSECURITY AND COMMUNICATIONS, NATIONAL PROTECTION AND PROGRAMS DIRECTORATE, U.S. DEPARTMENT OF HOMELAND SECURITY; CHERI FLYNN MCGUIRE, VICE PRESIDENT, GLOBAL GOVERNMENT AFFAIRS AND CYBERSECURITY POLICY, SYMANTEC; IAIN MULHOLLAND VICE PRESIDENT, ENGINEERING TRUST AND ASSURANCE VMWARE, INC.; CRISTIN FLYNN GOODWIN, ASSISTANT GENERAL COUNSEL, CYBERSECURITY, MICROSOFT CORPORATION; DEAN C. GARFIELD, PRESIDENT AND CEO, INFORMATION TECHNOLOGY INDUSTRY COUNCIL

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:]

******** INSERT 1-1 ********

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/Fin-Fisher 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:]

******** INSERT 1-2 ********

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:]

******** INSERT 1-3 ********

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:]

******** INSERT 1-4 ********

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 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 employees 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:]

******** INSERT 1-5 ********

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, an 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.

RPTR GENEUS

EDTR ROSEN

[3:22 p.m.]

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:]

******** INSERT 2-1 ********

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:]

******** INSERT 2-2 ********

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 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.

[The information follows:]

******** COMMITTEE INSERT ********

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 software, 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 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 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 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 of security providers 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 question 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.

[The information follows:]

******** COMMITTEE INSERT ********

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 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," end quote, 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 yields, 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.

RPTR MAAR

EDTR ROSEN

[4:23 p.m.]

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.

[The information follows:]

******** COMMITTEE INSERT ********

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.]