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

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

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

Introduction

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

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

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

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

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

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

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

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

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

My testimony will focus on four areas:

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

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

a. Defining the Problem

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

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

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

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

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

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

b. Defining Controls Related to Intrusion Software

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2. Impact of the Current Approach on Innovation and Cybersecurity

a. How Microsoft is Impacted by the Current Wassenaar Approach

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

d. Impact on Congressional Priorities

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

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

e. *Global Challenges Arising out of Wassenaar Implementation*

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

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

3. The Public Private Partnership and Cybersecurity Regulation

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

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

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

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

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

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

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

b. The Public Private Partnership, Cybersecurity and Export Control

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

4. Cybersecurity and Changing Global Norms

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

[17] *See* BSA Overview at 12.

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

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

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

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

5. Conclusion

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

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

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

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

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: Cristin Flynn Goodwin

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

   I have not received any federal grants, subgrants, contracts or subcontracts.

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

   I am testifying on behalf of my employer, Microsoft Corporation, where I am Assistant General Counsel for Cybersecurity in Microsoft's Trustworthy Computing division. In this capacity I lead Microsoft's Government Security Program (GSP) providing security support to governments. I also provide legal counsel to Microsoft's businesses and teams on a wide range of cybersecurity issues.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

   Microsoft Corporation does business with almost every federal agency. To the best of my knowledge, Microsoft does not receive grants or subgrants from the federal government. Microsoft does have some direct consulting and product support contracts with the federal government. However, most of Microsoft's business with the federal government, in particular software and online services, is conducted through reseller channels where Microsoft serves as a subcontractor under agency-wide agreements, the GSA Schedule or similar contract vehicles.

I certify that the above information is true and correct.

Signature:

Date: 1/7/2016

Cristin Flynn Goodwin is the Assistant General Counsel for Cybersecurity in Microsoft's Trustworthy Computing division. Cristin leads Microsoft's Government Security Program (GSP) which provides governments with a structured, legal means to access source code and affirm there are no back doors in Microsoft products or services, as well as to share information about threats and vulnerabilities. She helped launch the GSP's Transparency Centers in June of 2014 to enable secure government access to source code in response to the Edward Snowden allegations. Since 2008, she has been Microsoft's lead counsel for all aspects of Microsoft's security incident response processes and security updates for over a billion customers around the world. Cristin also provides legal counsel for Microsoft's cyber security public policy worldwide, supporting her clients and legal and policy experts in Microsoft's subsidiaries worldwide.

Cristin joined Microsoft in 2006, where she initially served as policy counsel in Microsoft's Washington, DC office. Prior to joining Microsoft, Cristin worked for BellSouth, and served in an operational role on a wide range of policy and operational issues, including during hurricanes Katrina, Rita, and Wilma in 2005, as well as Charley, Frances, Ivan and Jeanne in 2004, in addition to other National Security Special Events.

Prior to joining BellSouth, Cristin was policy counsel at MCI, where she specialized in cyber security, backbone network security and infrastructure protection issues, and was actively engaged in MCI's response to 9/11, and the myriad of policy, technology and legal work that ensued with the Federal government in the years following 9/11. Cristin began her career as a trial lawyer in New York City.

Cristin currently lives in Redmond, Washington with her husband and two children.