Testimony for the Record

Iain Mulholland

Vice President, Engineering Trust and Assurance

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Oversight and Government Reform's Subcommittee on Information Technology, and the Committee on Homeland Security's Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies

"Wassenaar: Cybersecurity and Export Control"

January 12, 2016

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

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

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

Concerns with the 2013 Wassenaar Arrangement

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

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

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

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

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

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

Examples of how Wassenaar Rules Could Undermine Cyber Posture

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

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

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

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

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

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

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

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

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

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

Next Steps

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

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

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

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

Summary

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

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

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

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

Name: **Iain Mulholland**

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.

Please see attached supplement.

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 VMware, Inc. I am the Vice President for Engineering Trust and Assurance at VMware.

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.

Please see attached supplement.

I certify that the above information is true and correct.

Signature: 

Date: 1/6/16

Attachment
Witness: Iain Mulholland
Representing: VMWare, Inc.

Disclosure Form for Witnesses
Committee on Oversight and Government Reform
U.S. House of Representatives

2015

Federal grant/contract	Federal Agency	Dollar Value	Subject of contract or grant
DJF153190P0010174	FEDERAL BUREAU OF INVESTIGATION	$0.00	ADP SOFTWARE
DJF153190P0010174	FEDERAL BUREAU OF INVESTIGATION	$3,811.04	ADP SOFTWARE
HHSP233201100186P	PROGRAM SUPPORT CENTER	($5,881.00)	OFFICE INFORMATION SYSTEM EQUIPMENT
DJF141100P0010702	FEDERAL BUREAU OF INVESTIGATION	($40.76)	ADP CENTRAL PROCESSING UNIT (CPU, COMPUTER), DIGITAL
TFSACFP150040	BUREAU OF THE FISCAL SERVICE	$5,085.00	EDUCATION/TRAINING- TUITION/REGISTRATION/MEMBERSHIP FEES
HHSP233201200123A	PROGRAM SUPPORT CENTER	($6,812.00)	ADP SOFTWARE
AID278O1400040	AGENCY FOR INTERNATIONAL DEVELOPMENT	$0.00	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
ING15PX00491	GEOLOGICAL SURVEY	$12,761.01	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
HHSI247201500024A	INDIAN HEALTH SERVICE	$13,804.80	ADP SOFTWARE

2014

Federal grant/contract	Federal Agency	Dollar Value	Subject of contract or grant
DJF142200P0003969	FEDERAL BUREAU OF INVESTIGATION	($299.95)	ADP SOFTWARE
AID278O1400040	AGENCY FOR INTERNATIONAL DEVELOPMENT	$5,101.16	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
INR14PX00886	BUREAU OF RECLAMATION	$0.00	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
HHSI247201400106A	INDIAN HEALTH SERVICE	$12,855.71	ADP SOFTWARE
INR14PX00886	BUREAU OF RECLAMATION	$24,501.60	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
N6660414P3373	DEPT OF THE NAVY	$1,995.00	EDUCATION/TRAINING- TUITION/REGISTRATION/MEMBERSHIP FEES
CNSIG14P0001	CORPORATION FOR NATIONAL AND COMMUNITY SERVICE	$21,312.06	IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
DJF141100P0010702	FEDERAL BUREAU OF INVESTIGATION	$166.60	ADP CENTRAL PROCESSING UNIT (CPU, COMPUTER), DIGITAL
S5105A11P0049	DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)	$409,366.00	ADP SOFTWARE
STH20014M1835	STATE, DEPARTMENT OF	$8,241.00	ADP SOFTWARE
DOLB149435567	OFFICE OF THE ASSISTANT SECRETARY FOR ADMIN AND MANAGEMENT	$9,945.90	ADP SOFTWARE
DJF142200P0003969	FEDERAL BUREAU OF INVESTIGATION	$299.95	ADP SOFTWARE
EP145000021	ENVIRONMENTAL PROTECTION AGENCY	$15,984.00	IT AND TELECOM- DATA CENTERS AND STORAGE

2013

Federal grant/contract	Federal Agency	Dollar Value	Subject of contract or grant
IND14PX00044	OFFICE OF POLICY, MANAGEMENT, AND BUDGET	$138,905.60	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
M6785409C4762	DEPT OF THE NAVY	$0.00	IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS
M6785409C4762	DEPT OF THE NAVY	$872,065.00	IT AND TELECOM- OTHER IT AND TELECOMMUNICATIONS
AIDOIGV1300295	AGENCY FOR INTERNATIONAL DEVELOPMENT	$4,151.00	TRAINING AIDS
S5105A11P0049	DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA)	$406,064.00	ADP SOFTWARE
CNSIG12P1228	CORPORATION FOR NATIONAL AND COMMUNITY SERVICE	$0.00	IT AND TELECOM- IT STRATEGY AND ARCHITECTURE
N0017313P1492	DEPT OF THE NAVY	$3,296.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
AG3144P130044	USDA, OFFICE OF THE CHIEF FINANCIAL OFFICER	$6,152.00	EDUCATION/TRAINING- OTHER
FTC13H3117	FEDERAL TRADE COMMISSION	$4,800.00	ADP SOFTWARE
N0016813P3706	DEPT OF THE NAVY	($1,875.30)	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES
HHSN263201300426P	NATIONAL INSTITUTES OF HEALTH	$4,965.28	ADP SOFTWARE
DOLB139A34461	OFFICE OF THE ASSISTANT SECRETARY FOR ADMIN AND MANAGEMENT	$34,307.30	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS
HHSD2002010M37509P	CENTERS FOR DISEASE CONTROL AND PREVENTION	$0.00	ADP COMPONENTS
N0016813P3706	DEPT OF THE NAVY	$0.00	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES
N0016813P3706	DEPT OF THE NAVY	$3,790.00	MEDICAL AND SURGICAL INSTRUMENTS, EQUIPMENT, AND SUPPLIES
N0017313P0523	DEPT OF THE NAVY	$0.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
DOCDG135010SU1761	NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION	$0.00	IT AND TELECOM- SYSTEMS DEVELOPMENT
N0017313P0523	DEPT OF THE NAVY	$4,000.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
N0018913PN064	DEPT OF THE NAVY	$16,754.00	MAINT/REPAIR/REBUILD OF EQUIPMENT- ADP EQUIPMENT/SOFTWARE/SUPPLIES/SUPPORT EQUIPMENT
W91QUZ12P0084	DEPT OF THE ARMY	$0.00	IT AND TELECOM- ANNUAL SOFTWARE MAINTENANCE SERVICE PLANS

Iain Mulholland, Vice President Research & Development, VMware

Iain Mulholland leads VMware's Engineering Trust and Assurance (ETA) group. Formed in early 2015, ETA focuses on ensuring customers continue to trust VMware products & services. ETA is a central engineering function within VMware's Research & Development organization comprising Product Security, a group which Mulholland built starting in 2011, Performance Engineering, Quality Systems and the Trust & Assurance team which focuses on Security Certifications, Software Supply Chain Security and the customer facing communication of VMware Trust & Assurance programs.

Prior to VMware he held senior leadership positions in several security and privacy early stage technology startups. A 20-year veteran of the software security space, Mulholland was an early member of the Microsoft Trustworthy Computing Group, where he led the Microsoft Security Response Center. A former British Army Officer, Mulholland is originally from Belfast, Northern Ireland but now calls Northern California home.