Iain Mulholland – Vice President, Engineering Trust and Assurance, VMware, Inc
Comments for ETRAC Meeting
October 15, 2015

I thank the Department of Commerce for allowing me to participate at the Emerging Technologies and Research Advisory Committee (ETRAC) Meeting to discuss the 2013 Wassenaar Arrangement.

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 allows 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, and computers and devices.

Thank you for the opportunity to provide our views on the Wassenaar Arrangement relating to export controls.

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 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 current 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. 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 with 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, against our customers infrastructures or business or government. This would only give malicious hackers an opportunity to exploit vulnerabilities knowing companies like ours would have our hands tied for an extended period of time while awaiting for export licenses to be applied for and approved.

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

1) As recently as this month, VMware collaborated with a small security research organization in Scotland to remediate a critical security vulnerability they had identified in one of our flagship products. This vulnerability, left unpatched, would allow a malicious attacker to take complete control of critical infrastructure. During the course of the investigation of this issue the researchers provided VMware with sample exploit code that demonstrated the flaw to VMware's Security Response team. This exploit code was key in accelerating the speed with which VMware's engineers were able to understand the flaw and develop a patch.

In this example the security researchers were in the UK, the coordinating VMware Security Response Center in the US and the team responsible for developing the patch in India. This would have necessitated 2 export license – one from UK to US and one from US to India. It is highly unlikely that a very small company based in the UK would have the means or inclination to get an export license in this scenario and even if they did this would have introduced delays of many days if not weeks. In all likelihood under the proposed Wassnaar rules this flaw would have gone unreported and customers would continue to be vulnerable to this critical security flaw.

This year alone, over half of the security vulnerabilities reported to the VMware Security Response Center from external parties have come from individuals or small 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. Security Researchers report security vulnerabilities to software vendors like VMware through a desire to make the Internet safer and there is no financial relationship between researchers and VMware. It is highly improbable that these small research companies or individuals will take on the administrative and financial burden of applying for export license 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 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 SAFECode, The Industry Consortium for Advancement of Security on the Internet (ICASI), and the Linux Foundation Critical Infrastructure Initiative. VMware regularly shares security information with participants of these forums and other forums. Indeed, security is often seen as a leveler and we often share threat information with competitors in an effort to ensure 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 this 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.

Moving forward, we recommend that BIS and the Department of Commerce keep all options on the table. This includes not only revisiting to improve its original proposal as a first step but also seriously considering returning to Wassenaar to renegotiate the original 2013 Arrangement. The reality is VMware, like other global technology companies, not only receive ever-dynamic cyber threat information 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 prevent network breaches, we must be able to act on a moments notice whether that information is coming from the U.S. or abroad. We must have the tools and resources on hand to act immediately.

In closing, VMware appreciates the opportunity to present our thoughts on this important issue. We hope that we were able to provide greater insight on the many challenges for a company, like VMware, to implement the 2013 Wassenaar rules. We stand ready to work in a constructive manner with BIS, the Commerce Department and other federal agencies to help resolve this issue. Thank you again for the opportunity.