Testimony for the Record

Iain Mulholland

Industry Member, Center for Strategic and International Studies

(CSIS) Cyber Policy Take Force;

Chief Technology Officer for

Security, VMware, Inc.

Before the

U.S. House of Representatives

Committee on Science and Technology Subcommittee on
Research and Technology

"Strengthening U.S. Cybersecurity Capabilities"

February 14, 2017

Chairwoman Comstock and Ranking Member and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Iain Mulholland, an industry member for the Center for Strategic and International Studies (CSIS) Cyber Policy Task Force; and Chief Technology Officer for Security at VMware Inc. I have nearly 20 years of 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 Microsoft, where in 2002, I was a founding member of the company's Trustworthy Computing Group.

My current employer, VMware, is a leading provider of software-defined solutions that increase the operation efficiency and security of data centers across the globe. Currently, VMware, is the fourth largest software company in the world with 2016 revenues of over $7 billion and over 19,000 employees. We are headquartered in Silicon Valley with 140 offices throughout the world, that serve more than 500,000 customers and 75,000 partners, including 100 percent of the Fortune 100. In addition to VMware's work throughout commercial markets, VMware remains committed to serving all sectors of the U.S. Government; including the Department of Defense, Civilian agencies, and the Intelligence Community, as well as state and local governments.

We are committed to enabling both government and commercial organizations with the ability to respond to their dynamic business needs, whether they utilize on premise datacenters, the cloud, or personal computers and mobile devices. VMware is providing enhanced security to government and commercial customers globally through its pioneering role in redefining how we build and secure networks, data centers, computers and devices.

Cybersecurity Policy

The U.S. Government is dependent on a vast cyber world of interconnected IT networks, data centers, the Cloud, mobile platforms, and other assets. Individual agencies rely on this cyber infrastructure to perform almost every mission critical function within their purview, from national defense and natural disaster response to postal services and the constitutionally mandated Census. In many cases, multiple agencies are interconnected at various operational levels to facilitate the sharing of business systems information and/or to provide interagency support to meet common mission objectives. The widespread adoption and use of cyber-systems has reaped immeasurable benefits for the country through increased government responsiveness, agency effectiveness, worker productivity, and a host of other economic efficiencies and returns.

Because we require cyber infrastructure to perform the modern-day functions of government, sophisticated and aggressive cyber-attacks perpetuated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. As you know, there have been well-publicized cyber-attacks, including one of the largest cyber-attacks on a U.S. agency, the Office of Personnel Management (OPM), which suffered one of the most damaging breaches of information ever on government workers. As this Committee knows, the OPM breach and the other federal agency attacks, have compromised the personal data and security of over 21 million current and former federal employees and has likely compromised our national security, national defense, and national intelligence posture(s). These breaches have put our nation's blood and treasure at risk.

We are also experiencing an unprecedented level of cyber-attacks and sophistication in the private sector. The reality is that global technology companies, like VMware, not only receive an unprecedented amount of information in regards to cyber threats from inside the U.S., but we also receive a large number from overseas as well. The fact is, with data moving across borders instantly, the digital devices and technologies associated with the ecosystem, and therefore cybersecurity, is not confined to physical 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.

Building on the 2009 Commission on Cybersecurity, the Center for Strategic and International Security established the Cyber Policy Task Force to lay out practical steps for policy, resources and organization that the next Administration can use to build better cybersecurity. The goals for a national approach to better cybersecurity remain largely the same: to create a secure and stable digital environment that supports continued economic growth, while protecting personal freedoms and national security. The requirements for implementation also remain the same: central direction and leadership from the White House to create and implement a comprehensive and coordinated approach to cybersecurity.

In the eight years since that report was published, there has been much activity and an exponential increase in attention to cybersecurity, however, we are still at risk and there is much for this current Administration to do.

Specifically, CSIS believes that there are five core areas that require renewed focus:

- First, the development of a new international strategy based on partnerships with like-minded nations, to improve the ability of deterring attackers, by developing a full range of response and countermeasures that go beyond the threat of military action.

- Secondly, there must be a serious effort to reduce cybercrime, with consistent Cabinet level support, to build international cooperation to fight botnets and sophisticated financial crime. Part of this effort must be to penalize countries that won't cooperate in the effort to reduce and control cybercrime.

- Thirdly, we must prepare our critical infrastructures and services for attack and improve "cyber hygiene." The new Administration should use incentives when possible, but be ready to regulate if incentives don't work. Greater use of shared, managed and cloud services can make government agencies more secure.

- Furthermore, we must identify where Federal action in resource issues, such as research or workforce development, is necessary, since many of these efforts are best left to the private sector. We don't need a cyber "Manhattan Project."

- And finally, we must streamline White House bureaucracy, increase oversight of Federal cybersecurity by creating a special GAO office*,* and clarify the roles of DOD and other agencies. A stronger DHS is crucial, and the new Administration must either strengthen DHS move the cybersecurity mission.

To build on the theme of increasing the cyber role of DHS, in the President's Commission on Enhancing National Cybersecurity Report published in December, one of the recommendations (5.1) was to consolidate basic network operations in the Federal Government. I agree with this recommendation, but only if network architecture is done the correct way with the proper security. In President Obama's Cybersecurity National Action Plan (CNAP), he expanded the Department of Homeland Security's EINSTEIN and Continuous Diagnostics and Mitigation (CDM) programs. As the Committee knows, these two programs were designed to detect, prevent and mitigate cyber incidents on the Federal Government's Civilian networks.

Originally conceived as a three-phased program, the FY17 Department of Homeland Security Budget request expanded the CDM program to add a Phase 4 in order to address the ever-changing cybersecurity landscape. This expands on CDM Phase 3, which primarily focuses on boundary protection, including data loss prevention, and incident response. CDM Phase 3 provides Federal civilian departments and agencies with the capability of identifying and protecting against anomalous activity inside Federal networks, as well as alerting security personnel for expedited remediation. CDM Phase 4 will expand the program to include additional tools and services that protect sensitive and high value asset data **within** agency networks.

These tools and services include programming that mimics current data stores (data masking), encodes data during its transfer (encryption), creates multiple compartments within a system for data storage (micro-segmentation**),** and only allows individuals with specific credentials to access and manipulate specific data (digital rights management), as well as deploys, secures, monitors, integrates and manages mobile devices, such as smartphones, tablets and laptops, in the workplace (mobile device management).

Microsegmentation Policy

I'd like to take a minute to highlight microsegmentation, a key part of the CDM Phase 4 program and explain why I believe it must be continued, expanded and accelerated to fully secure government networks.

VMware testified before this Committee last year to discuss the best practices that the government could adopt to lessen cyber threats. Let's take the Office of Personnel Management (OPM) breach as an example again. As is apparent from publicized accounts, the nature of the security breach at OPM is not particularly unique. Hackers were able to penetrate perimeter network security systems and subsequently gain access to OPM systems, where they were free to roam around the internal network and steal sensitive data over a period of several months. Hackers typically use this attack methodology because traditional perimeter-centric security systems are structurally designed to be "doors" to the network. These doors serve to allow authorized users access to networked systems and to prevent unauthorized users from getting inside a network. However, structurally the perimeter is the single point of failure (a single perimeter: firewall + additional security systems like intrusion prevention or advanced attack detection) that must be breached in order to enter the data center network. Once the intruder has penetrated perimeter security, there is no simple means to stop malicious activity within the data center without extreme disruption to the agency's mission. In many cases, the response from agencies and network security vendors is to add more security technology to the perimeter – which ignores the structural issue.

VMware submits three salient points for consideration:

1) Every recent agency breach has had one thing in common: the attacker, once inside the perimeter security, has been able to move freely around the agency's network.
2) Perimeter-centric cyber security policies, mandates, and techniques are necessary, but alone they are insufficient and ineffective in protecting U.S. Government cyber assets.
3) These cyber-attacks will continue – but we can greatly increase our ability to prevent them, and limit the damage and severity of the attacks when they do.

There are lots of perimeter-centric technologies that are designed to stop an attacker from getting inside a network – clearly this approach is not sufficient to combat today's cyber-attacks. Perimeter-centric security solutions are analogous to a locked door that can only be accessed with a key. The primary function of the door is to deny initial unauthorized entry by anyone that does not have a key. However, once the door is forced open (hacked or breached), the unauthorized actor is free to move throughout (laterally) unabated.

In order to effectively prevent an Attacker from moving freely around the network, agencies must compartmentalize their networks by creating "zero-trust" or "micro-segmented" network environments within the data center. A zero-trust environment prevents unauthorized lateral movement within the data center by establishing automated governance rules that manage the movement of users and data between business systems and/or applications within the data center network. When a user or system "breaks the rules", the potential threat incident is compartmentalized and security staff can take any appropriate remediation actions. To build on the analogy above, compartmentalization is equivalent to securing each interior room with locks. Only those with the appropriate keys can move freely within the data center. The magnitude of a perimeter security breach, or break-in, is significantly mitigated by limiting the intruder's ability to move around freely within the house.

In an era of constrained resources and imminent threat, the old perimeter based approach is insufficient and untimely. Congress last year did not fully fund CDM Phase 4 due to budget constraints. We would urge this Committee's strong support for full and accelerated funding for the Einstein and CDM programs.

IoT Security

I'd also like to touch on another topic that is important to securing the cyber eco-system, the Internet-of-Things (IoT).

We are at the cusp of the Internet-of-Things, the Internet of Everything, where we have an intelligent world connected in almost every aspect of our daily lives. From our health care to manufacturing to banking to home monitoring, and now into "smart cities", transportation and the list goes on. IoT has been called by some as "the next Industrial Revolution." In fact, several recent studies, including a recent Business Insider survey, estimate that "there will be 34 billion devices connected to the Internet by 2020, up from 10 billion in 2015. IoT devices will account for 24 billion, while traditional computing devices (i.e. smartphones, tablets, smartwatches, etc) will comprise of 10 billion."

Due to this increasingly interconnected economy, there is no doubt that "security" is the linchpin for the advancement of IoT technologies. We have seen the impact and vulnerabilities from the October DDoS attack that targeted many older, outdated devices, devices that did not utilize any of the industry's standard best practices for cybersecurity.

Consumers, businesses and Government need to feel confident that IoT technologies are secure and their privacy is protected. At VMware, we have launched Liota (Little IoT Agent), a vendor neutral Open Source software development kit for building secure IoT gateway data and control applications.

A way to secure the IoT ecosystem is by ensuring flexible and isolated connection points through secure manageable infrastructure, such as edge systems, which include, but not limited to, IoT gateways. Whenever an IoT device connects to the Internet, whether by itself or through an IoT gateway, that system needs to be manageable, deployed responsibly with a proper initial configuration, and maintained at the current state of best-security-practices available throughout the complete lifetime of the device.

IoT gateways are an integral part of the IoT infrastructure. They bridge, but also decouple, the physical IoT devices from management components in data centers. This bridge allows data and control to move freely and securely from the device to the cloud or data center. We will need secure IoT Gateways to ensure data and information are secured as it moves through the IoT pipeline.

As Congress and the Administration continue to work on policies promoting the IoT economy, we believe that some consideration should be given to developing some rules of the road type standards for IoT moving forward. Absent any Federal action around IoT, standards could be developed in divergent and potentially disruptive ways. Among others, we would agree with a CSIS recommendation calling on NIST and other federal agencies to cooperate with industry stakeholders in order to develop a set of standards and principles for IoT security.

Wassennaar

Another cybersecurity issue looming that could have a significant impact on the cyber ecosystem is the 2012 Wassenaar Arrangement.

The Wassenaar Arrangement was originally established over 20 years ago and now includes 41 nations to promote transparency and responsibility in transfers of conventional arms and dual-use goods and technologies. In 2013, the Wassenaar Plenary, seemingly expanded its original mission beyond regulating technologies that could be incorporated into conventional weapon systems, to include regulating the export of certain types of equipment, software and technology used to distribute or produce malicious “intrusion software.” We know that the two capabilities demand two separate and unique skill sets. Regulating conventional weapons and arms requires a very unique expertise, much different from the expertise required to develop, code and patch software.

In short, the 2013 Wassenaar rules would severely impact the ability of the U.S. technology industry 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 ultimately, less security for customers and the global cyber ecosystem.

Last year, to their credit, the U.S. government recognized that it needed private sector technologists at the negotiating table to help renegotiate the “software intrusion” provisions included in the 2013 Wassenaar Arrangement. I was invited to join the U.S. Delegation in Vienna during the June and September Wassenaar Sessions with the goal of providing U.S. technology and security industry expertise directly at the negotiating table. This was the first time that the U.S. Delegation included non-government cyber experts at the September meeting, due to niche knowledge we provide as security practitioners.

That said, the new Administration faces an ever-increasing amount of challenges in securing cyberspace. Attacks are on the rise and massive numbers of interconnected devices threaten to overwhelm Internet defenders. Cyber export control agreements have been drafted in the past several years, and the importance of getting them right affects not just national security, but the entire global Internet ecosystem. Getting them wrong means crippling Internet defenders.

It is my hope that the new Administration will continue to view this as a leadership opportunity for the U.S. to shape international cyber norms and support the ongoing renegotiations on the Wassenaar Arrangement. The continued US renegotiation efforts, in partnership with the U.S. technology industry and bipartisan support from Congress, can ensure a sound Wassenaar Cyber Agreement that enhances our nation's cyber posture and ultimately strengthens our defense against attacks.

Summary

As I mentioned in my testimony, the global digital ecosystem is experiencing an unprecedented level of cyberattacks and sophistication. 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. As laid out in my testimony, CSIS proposes a series of recommendations that Congress and the Administration should consider to reduce the threat of cybersecurity on federal and commercial networks.

Promoting good cyber hygiene should also be a key standard that helps agencies, consumers and businesses better protect their information and networks from hackers. One of the best ways for the Federal Government to be pro-active is by deploying microsegmentation technologies that offer the ability to segment their networks in the event of a breach.

Additionally, as part of enhancing the global cyber eco-system, we must ensure that devices and technologies associated with the Internet-of-Things (IoT) are secure for consumers, businesses and the federal government. Security is the key principle that will enable and advance further adoption in IoT. Congress and the Administration should look to develop reasonable standards around IoT security moving forward.

Lastly, I would like to encourage the new Administration to continue to seek reasonable improvements to the 2013 Wassenaar Arrangement. The U.S. has an opportunity to demonstrate global leadership to craft new international cyber agreements in the future. The new Administration should continue the negotiating efforts at Wassenaar moving forward.

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