Testimony for the Record

Ray O'Farrell

Chief Technology Officer

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Oversight and Governmental Reform Committee

"Cybersecurity of the Internet of Things"

October 3, 2017

Chairman Hurd, Ranking Member Kelly, and Members of the Committees, thank you for the opportunity to testify today at this important hearing. I am Ray O'Farrell, executive vice president and chief technology officer at VMware Inc; and head of VMware's Internet of Things business unit. I have nearly 30 years of experience in the software engineering field, primarily in embedded systems and secure, robust infrastructure software.

VMware is a leading provider of software-defined solutions that increase the operational efficiency and security of data centers within the federal government and across the globe. Currently, VMware is one of the largest software companies in the world with 2016 revenues of over $7 billion and more than 19,000 employees. We are headquartered in Silicon Valley, California, with 140 offices throughout the world, serving more than 75,000 partners and 500,000 customers, including 100 percent of the Fortune 500. The U.S. government is a long standing critical partner and customer of VMware and we remain 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. VMware is a part of the Dell Technologies family of companies, which is the largest privately controlled technology company in the world.

We are committed to providing both government and commercial organizations with the ability to respond to their dynamic business needs, whether they utilize on-premises 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 cyberworld of interconnected information technology (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 immeasurably benefitted 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 cyberattacks perpetrated 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 cyberattacks, including the Office of Personnel Management (OPM) breach, which compromised the personal data and security of over 21 million current and former federal employees.

We are also experiencing an unprecedented level of cyberattacks in the private sector. As an example, in recent weeks the well-publicized security breach of a large credit reporting agency creates the potential that the personal data of well over a hundred million of United States citizens has been potentially compromised. This summer several ransomware attacks including WannaCry crippled the operations of a major global shipping company, one of the largest package delivery companies, a major drug manufacturer, as well as several healthcare providers. The reality is that global technology companies, like VMware, in cooperation with our customers observe a constantly growing increase both in incidence and sophistication of cyberattack – both from and upon systems inside the U.S. and overseas.

Internet of Things (IoT) Security

The emergence of the Internet of Things (IoT) is a technological step in which more and more aspects of the physical world, from manufacturing to banking to home monitoring to healthcare, transportation and even "smart cities" are interconnected and coupled with analytics and intelligence. The insights gained drive increased performance and efficiency of our infrastructure and bring new services to almost every aspect of our daily lives. Some consider IoT to be "the next Industrial Revolution." Unlike most traditional computing devices, many of these IoT Things will be directly connected to important physical aspects of our lives – from smart meters to factory robots, from cars to traffic lights, and even to devices in our own bodies such as insulin pumps and pacemakers. We will see a significant increase in IoT Gateway devices that aggregate and manage large collections of IoT devices in close proximity to the IoT device. These IoT Gateway devices are often powerful with some datacenter-like characteristics but will be deployed well outside the safety of traditional physical datacenter boundaries – in cars, on oil rigs, as part of the power grid, in factories, on cell towers. Indeed, several recent studies, including a recent Business Insider survey, estimate, "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 10 billion."

This level of interconnect will lead to exciting new capabilities in our ability to manage and optimize the infrastructures of our country, from manufacturing, to transportation systems, water management systems and many others – but also makes it critical that we secure the IoT from those with malicious intentions.

- It is vital, that we secure IoT infrastructure to prevent the compromise or disruption of our economy. This infrastructure, which among other things, will now form the basis of how factories and cities critical infrastructure interfaces with the real world.

- Securing these devices before they can be used as entry points or vectors to attack other parts of cyber infrastructure is paramount to overall strong cyber security.

The threat and impact of IoT based cyberattack is not theoretical; it is real. We have seen the impact and vulnerabilities from last year's distributed denial-of-service (DDoS) attack targeting outdated devices that did not correctly utilize the industry's standard best practices for cybersecurity. That attack took down major internet platforms and disrupted internet services for millions of Americans. The major wave of ransomware attacks this summer that wreaked havoc in the industrial, healthcare and logistics sectors were enabled in part by vulnerable devices that were not built securely or with patching in mind.

Importance of Cyber Hygiene

While there is certainly no silver bullet or single solution to prevent cyber-breaches generally or within IoT specifically, we believe that many of major breaches in the last few years would have been dramatically reduced or entirely eliminated if some fundamental principles of cyber hygiene had been followed. We propose five core cyber hygiene principles (below) as a universal baseline: the most important and basic things that organizations and the federal government should be doing. The concepts are not new but are key in moving to more effective security. They are rooted in well-established frameworks such as the NIST Cybersecurity Framework (CSF) and are technology-neutral.

1. Least Privilege	If a least-privilege environment has not been effectively implemented and users are provided with higher levels of access than they need, attackers can steal these users' credentials (user name and password) and gain broad access to systems. For example, it is understood, in the Target and Sony breaches, attackers were easily able to gain administrative-level privileges.
2. Micro-segmentation	If micro-segmentation has not been effectively implemented, attackers can break into one part of the network and then easily move around to other parts. For example, it is understood, in the Target breach, after an initial intrusion into the HVAC system, the attackers were able to move around to the payment network system. In the Sony breach, the attackers were also able to move around from one part of the network to another. In the case of the OPM breach, the attackers obtained access to OPM's local area network and then pivoted to the Interior Department's data center.
3. Encryption	If encryption has not been effectively implemented, attackers can exfiltrate data in readable form. For example, it is understood, after a data breach at Royal & Sun Alliance Insurance PLC, government investigators determined that the company had not adequately encrypted the data.
4. Multi-Factor Authentication	If multi-factor authentication (MFA) is not effectively implemented, attackers can obtain passwords and use them to access systems. For example, it is understood, in the OPM breach, if the contractor log-ons had been enforced with a risk-appropriate level of MFA, it would have limited the ability of the attackers to use the stolen credentials of the government contractor. In the case of the breach at LinkedIn, the hack exposed inadequately protected passwords of 100 million users. Since consumers often use passwords on

	multiple sites, MFA would have reduced the risk.
5. Patching	If patching is not effectively implemented, attackers can exploit open holes in systems. For example, it is understood, the ransomware attacks such as WannaCry exploited known software vulnerabilities for which patches were available. Organizations that fell victim had failed to effectively patch.

With education firmly in place, these five pillars of cyber hygiene are key in moving to more effective security.

VMware's Vision on IoT

Because VMware is the leader in datacenter and IT infrastructure management, we have a unique perspective on ways to secure the IoT ecosystem. With the advent of the Internet of Things, as more and more connected things are added to your network, it is a natural evolution of VMware's capabilities to now go out to the edge and help IT manage this new infrastructure.

Consumers, businesses and government need to feel confident that IoT technologies are secure and their information is protected. At VMware, we have advanced IoT products and software applications that embed each of the five cyber hygiene principles laid out earlier.

A way to secure the IoT ecosystem is by ensuring flexible and isolated connection points through secure manageable infrastructure, such as 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 securely from the device to the cloud or data center. We need secure IoT Gateways to ensure data and information are secured as it moves through the IoT pipeline.

The Internet of Things (IoT) Cybersecurity Improvement Act of 2017

As Congress and the Administration continue to work on policies promoting the IoT economy, we believe that it is important to seek input from industry stakeholders. Security needs to be paramount to protect sensitive data and information, as well as securing critical infrastructure. We believe it makes sense for NIST and other relevant federal agencies to cooperate with industry stakeholders in order to develop a set of standards and principles for IoT security. This is equally, if not more important, when federal agencies purchase IoT devices.

VMware applauds Senators Warner (D-VA) and Gardner (R-CO) for their bipartisan leadership in crafting the Internet of Things (IoT) Cybersecurity Improvement Act of 2017. We believe that the proposal is innovative when it comes to IoT security. We also commend the Committee leadership for releasing a Discussion Draft of the Senate proposal to seek additional stakeholder input.

There are several provisions of the proposal that VMware specifically supports. For example, we believe IoT devices should, from the outset, be designed with vulnerability patching capabilities built-in. A simple patching requirement could have drastically reduced or eliminated the WannaCry and similar ransomware attacks. In addition to the patching requirement, we support several of the cyber hygiene concepts in the proposal, which include micro-segmentation and multi-factor authentication. The concept of micro-segmentation would play a critical role in ensuring that IoT related data and information are segmented and properly protected against IoT cyberattacks. This would go a long way in providing additional layers of security to protect sensitive data and information in the IoT ecosystem. We also support the security considerations included in the proposal that would be provided by IoT gateways. If an IoT device lacks a minimum level of patching security, requiring systems like IoT Gateways would provide an appropriate layer of security protection for consumers, businesses and the federal government. IoT Gateways are embedded with many of the core cyber hygiene principles such as least privilege, micro-segmentation, patching, multi-factor authentication and encryption.

In all, the **Internet of Things (IoT) Cybersecurity Improvement Act of 2017** is an important, bipartisan step forward in promoting a secure federal IoT ecosystem.

Summary

The global digital ecosystem is experiencing an unprecedented level of sophisticated cyberattacks. In order to secure and adequately protect our customers, products, services, and networks against these highly sophisticated attacks, we must utilize every security tool we have in the toolbox. The IoT economy presents a significant opportunity for U.S. companies. Billions of IoT-connected devices will be on the free market for consumers, businesses, and government to consider purchasing. The U.S. has a ripe opportunity to claim global leadership in the IoT space. The IoT economy will create American jobs and could be an opportunity to boost American manufacturing across the country.

The IoT economy will also provide new efficiencies for consumers, schools, hospitals, and manufacturing, as well as federal, state and local governments. Security is the key principle that will enable and advance further adoption of IoT. If consumers, businesses and government do not feel that IoT products are secure, it will only hinder U.S. global leadership in an inevitably growing and innovative IoT economy.

Promoting good cyber hygiene should also be a key goal that helps agencies, consumers and businesses better protect their information and networks from malicious attackers. One of the best ways for the Federal Government to be proactive is by deploying micro-segmentation technologies that offer the ability to segment their networks in the event of a breach.

The **Internet of Things (IoT) Cybersecurity Improvement Act of 2017** provides a thoughtful framework, modeled after the industry-recognized NIST framework, for the federal government to put forth some baseline security recommendations to consider when specifically purchasing IoT-related and edge-computing devices. We are pleased that the proposal includes important cyber hygiene concepts, such as patching, micro-segmentation and multi-factor authentication. We also support the considerations included in the proposal that leverage the security benefits introduced by properly managed IoT gateways, which can act as isolation and management gateways to help prevent and remediate any comprise of connected devices. VMware commends Senator Warner and Senator Gardner for introducing this legislation, and we applaud the efforts of the Committee for putting forth the discussion draft for additional stakeholder input.

I appreciate the opportunity to share my thoughts on this very important issue. We applaud the leadership and vision of Chairman Hurd and Ranking Member Kelly for holding this hearing. VMware looks forward to continuing to work with the Committee on this and other important issues. Thank you again for the opportunity.