Statement for the Record

Dominick (Dom) Delfino, Vice President

World Wide Systems Engineering

Networking and Security Business

VMware, Inc.

Before the

U.S. House of Representatives

Committee on Armed Services

Outside Perspectives on the Department of Defense Cyber Strategy

September 29th, 2015

Chairman Thornberry, Ranking Member Smith, and Members of the Committee, thank you for the opportunity to testify today. I am Dominick (Dom) Delfino, Vice President of World Wide Networking and Systems Engineering at VMware.

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 DoD Cyber Strategy released in April.

Cyber-Attacks: Clear and Persistent Threat to the U.S. Government

The U.S. Government depends 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 perpetrated by criminal entities and foreign government agencies represent a clear and persistent national security threat to the U.S. Government. Recent well-publicized cyber-attacks have targeted the Department of Defense, the Office of Personnel Management, U.S. Postal Service, the U.S. State Department, the Internal Revenue Service, and other agencies.

Department of Defense Cyber Strategy

Goal 1: Build and maintain ready forces and capabilities to conduct cyberspace operations

We believe that DoD's Cyber Strategy is a good first step towards improving the Department's cyber posture. Providing our cyber warriors with the skills to fight this battle is a challenge due to the variety of constant changing threats and missions they face on a daily basis. VMware believes that this challenge, while seemingly daunting, can be managed with a few industry proven practices.

1. Realistic and robust simulated cyber-training environments are needed to effectively develop and test the skills of cyber warriors. Current methods for engaging the cyber threat require high levels of training on complex tools and costly security products. By applying currently available technology, these environments can be built on demand, represent the evolving threat and not require an army of support contractors. Once in place, these cyber classrooms can provide on-demand training to warfighters globally. VMware has worked with organizations such as the Ft. Gordon Cyber Leadership School to pilot these capabilities with promising results.
2. We recommend DoD leverage currently available automation technologies and simplify the cyber detection and course of action. By creating push-button responses that can be just as rapidly undone, the Department can empower today's cyber warriors with the ability to stop threats immediately, even temporarily, without having to wait for a complex change process. Today, to deploy a cyber countermeasure such as blocking an attacker or modifying a firewall, is a timely and complex process that takes hours or days when every minute counts. With automation, more on demand, yet immediate countermeasures can be deployed to stop specific threats. With this capability DoD can

rapidly expand the courses of action without requiring years of training on complex tools. This would allow current experts to automate simple countermeasures and reserve the best and brightest cyber warriors for the most significant threats such as searching for unexploited vulnerabilities and developing tactics and techniques.

The United States Government, the DoD as well as other agencies responsible for dealing with cyber security should undertake a significant initiative to attract, recruit, retain and train a talent pool to stay at the forefront of cyber security knowledge. Attracting the right talent is one of the most challenging aspects of creating a cyber defense operation. My suggestions are as follows:

1. The U.S. Government, and more specifically the DoD, has the ability to be competitive with private sector for cyber talent, but it must be creative in its tactics and use programs like the special hiring authority which allows agencies to pay a higher wage for experienced personnel with specialized skills. The DoD should consider a blend of civilian employees, military personnel and contractors.
2. Require ongoing training and development and create a cyber promotion path. Technologies and threats evolve rapidly today. Cyber skills need to be updated frequently in order to stay ahead of our adversaries. Personnel in this field should receive one full week of training per quarter inclusive of Industry and DoD relevant certifications and accreditations. DoD may also want to consider creating a career track so that cyber warriors have promotion paths to command level responsibility.

Goal 2: Defend the DoD information network, secure DoD data, and mitigate risks to DoD missions

As the Department is implementing its new Cyber Strategy, security should not only focus on the perimeter because the current approach it is not working. We know the threat landscape is constantly evolving; as soon as one vulnerability is mitigated, another threat vector arises. The attackers deal strictly with software that is being written, updated, and refined on a daily basis and this fact puts our agencies at a tactical disadvantage on a daily basis. Government networks that rely on a traditional hardware-based perimeter security strategy will never be able to keep pace with an ever-changing software-defined world.

The recent attacks on our Government have had one thing in common: the attacker, once inside the network perimeter security, was able to move freely around the victim's network. It is clear to our nation and to those who perpetrate these attacks that the way in which we protect our national cyber infrastructure, and the way in which most federal entities and agencies design and deploy cyber security systems is ineffective.

Too much trust is placed on perimeter-based security and human responses to secure networks. As history has shown, this approach leaves our nation vulnerable and at a significant disadvantage. Hackers were able to penetrate perimeter network security systems and subsequently gain access to systems where they were free to access 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, the structure of perimeter-based security makes it 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; this response ignores the structural insufficiencies.

Mitigating the economic, political, and social damage to our nation from these types of cyber-attacks demands that we change the way we build, operate, and secure our Government’s mission critical IT infrastructure.

VMware submits three salient points for consideration:

1) Every recent agency and private sector 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. This is a fundamental flaw of network architectures that have proliferated over the past 15 years. The hackers are aware of this flaw and leverage it extensively once inside the network infrastructure.

2) Perimeter-centric cyber security policies, mandates, and techniques are critical and necessary, but they are insufficient and ineffective in protecting U.S. Government cyber assets alone.
3) These cyber-attacks will continue, but it is possible to significantly and affordably increase our prevention abilities and limit the damage and severity of attacks.

Address the Threat – Immobilize the Attacker

There are many perimeter-centric technologies designed to stop an attacker from getting inside a network, however it is evident that 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 another example, imagine a street containing several homes as an analogy for a network containing several servers in a data center. Let's further imagine that there is a corridor that connects every home on the street. If an intruder can manage to break into one home, the intruder now has complete access to all of the other homes on the street even though the doors to the street are locked because there is a trusted passage between them. If the street is long and contains many homes, it has a higher probability that an intruder will be able to access one of those homes and leverage the trusted corridor to access and rob every home on the street, and potentially other streets in the neighborhood. In technology terms, the larger and "flatter" the network, and the more servers on the network, the higher the probability the intruder or hacker will be able to penetrate one server and leverage it to compromise others on that same network. This is what has occurred in most of the private and government cyber attacks in recent months.

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, and the "trusted corridor" is now no longer trusted, and it becomes monitored by automated "guards" who systematically check for and verify correct credentials. Limiting the intruder's ability to move around freely within the house or through the corridor significantly mitigates the magnitude of a perimeter security breach, or break-in.

While many information technology departments have network segmentation initiatives under way, they are largely insufficient because they use a legacy approach. This legacy approach involves attempting to move perimeter security inside the data center. While these entities tend to achieve some level of segmentation or separation between networks, it is both costly and has limited scalability. In my experience, I find that these organizations discover that this legacy approach does not scale well and becomes overly complex and operationally infeasible. Ironically it leads to reduced security over time. Rather than this legacy approach, a Zero Trust security model should be implemented. This model states that security professionals must eliminate the idea of an internal trusted network and an external untrusted network. In a "zero trust network" all networks are untrusted, meaning there is no "trusted corridor."

Three concepts underpin "Zero Trust: 1) verify and secure all resources regardless of location, internal or external; 2) limit and strictly enforce access control across all user populations, devices, channels and hosting models; and 3) automatically log and inspect all traffic, both internal and external. This can be automated and performed seamlessly without negatively impacting user response time on the network.

Build the Joint Information Environment (JIE) single security architecture

General Keith Alexander (USA, Ret.), former Director of the National Security Agency and Commander, U.S. Cyber Command, has repeatedly warned of the threats to DoD's networks: *I look at the DoD Architectures today, and defending them is really hard. We have 15,000 enclaves, each individually managed. The consequence of that is that each one of those is* *patched and run like a separate fiefdom. The people who are responsible for defending them cannot see down beyond the firewalls. Host-based security systems are helping, but practically speaking, Situational Awareness (SA) is non-existent.* [1]

As the Committee is well aware, the Pentagon is building the Joint Information Environment (JIE), a single joint enterprise IT platform that can be leveraged for all DoD missions. It is designed to provide greater standardization and end-to-end visibility with a new single security architecture. We applaud the Department's effort to move to the JIE as it provides a sound framework for enhancing DoD's security posture.

A key recommendation for a successful migration is to leverage the existing cloud based technologies that DoD owns and is in the process of deploying, allowing them to slowly consolidate workloads into the JIE framework. For example, the Air Force is currently leveraging cloud technology to standardize and automate multiple data centers. The Department may want to consider implementing a scorecard to measure and manage the Commands that are making progress to achieve JIE alignment, and leverage their best practices across DoD.

As the Department is implementing its network defense across the enterprise, it should review how it treats unclassified business system networks. Currently these systems, such as email, personnel, and payroll are treated differently than mission critical systems under current DoD practices. As we have seen by recent cyber-attacks on these systems, multiple vulnerabilities on different levels of systems exist today. While many systems may not be deemed mission critical, the impact of a cyber attack on these systems can be just as effective in impairing our ability to defend our nation. Let's assume for a moment that the DoD payroll system was compromised. What would the impacts to troop moral and effectiveness be when their families are not getting their paychecks? These scenarios demonstrate the need for action to ensure all systems are protected. There are proven technologies that can provide the DoD agile tools that can be deployed rapidly in hours or even minutes that can adapt dynamically to the threats. VMware as well as other technology vendors are delivering these technologies to IT companies and the military today.

[1] General Keith Alexander (USA), USCYBERCOM Commander and Director of NSA, "Interview to Federal News Radio," August 24, 2012.

Goal 3: Be prepared to defend the U.S. homeland and U.S. vital interests from disruptive or destructive cyberattacks of significant consequence

We recommend two approaches in addressing these initiatives. The first is to automate security features. This will allow the Department to rapidly and dynamically change the countermeasures in place during high threat periods. As stated earlier in my testimony, Zero Trust models are a good example of the security features that can be put into place automatically and used on demand.

The second approach is to use predictive methods to quantify attacks and likely actions based on their early stage. This "cyber kill chain" helps to identify and predict an attacker's next move. Investing in these capabilities will yield significant benefits by preventing later stage and more serious attacks based on the precursor activities. However, the benefit of these approaches will be reduced if not coupled with on-demand controls and empowerment of our cyber warriors on the front line to use them. This approach can make our cyber defense forces more effective at preventing serious compromises by detecting and stopping these early stage attacks or diverting them to specialists for offensive actions.

Summary

VMware is committed to supporting the U.S. Government's defense of our national cyber infrastructure. VMware understands the Department's challenges in addressing the persistent cyber security threat. New cyber security strategies (e.g. Zero Trust or micro-segmentation) that are the current gold standard for commercial industry must become the gold standard for the Department of Defense. To facilitate adoption, government policies should establish ratio metrics for the number of systems/workloads a given system has access to without passing security controls. Today, most government networks have a ratio of 1 to hundreds or 1 to thousands. The target ratio should be 1 to ones or 1 to tens so that if a given network is breached, the damage will be greatly limited. Metrics will enable government policies to better address today's cyber warfare reality. Additionally, these controls can be adapted dynamically and often automatically to the threat level.

While there is no “silver bullet” to permanently address every cyber security threat, Congress can mandate that agencies adopt policies and security standards that mitigate threats inside the network perimeter.

In summary, the Department of Defense should:

1) Establish aggressive automation goals for the management of their IT infrastructure that includes security controls.
2) For all existing networks, cut the common thread found in every major breach by implementing a Zero Trust security model and reducing attacker/threat mobility within the network.
3) Reward successful organizations when moving to the JIE by sharing best practices within DoD.

VMware sincerely appreciates the opportunity share our thoughts and suggestions on this very important matter. We applaud the leadership and vision of the Chairman and Ranking Member in holding this important hearing. VMware looks forward to continuing to participate in efforts to improve the security of the federal government. Thank you for the opportunity to testify today.