Prepared Testimony and
Statement for the Record of

Kenneth Schneider
Vice President & Fellow
Symantec Corporation

Hearing on

"Cyber Security: What the Federal Government Can Learn from the Private Sector"

Before the

United States House of Representatives
Committee on Science, Space, and Technology
Subcommittee on Research and Technology
and
Subcommittee on Oversight

January 8, 2016

Chairwoman Comstock, Chairman Loudermilk, Ranking Members Lipinski and Beyer, my name is Ken Schneider. I am the Vice President of Technology Innovation at Symantec where I focus on innovation, strategic investment and aligning our security technology development vision to our strategy. I am also a Symantec Engineering Fellow, one of a select group of employees who have been recognized as Symantec's top experts in a specific field. Prior to joining Symantec, I was the Chief Technology Officer and Vice President of Operations for Brightmail, an anti-spam software company that was acquired by Symantec in 2004. Before that I founded South Beach Software, a software and consulting company that developed products for the professional video market, and also acted as an independent software consultant for clients including Sun Microsystems and Digital Equipment Corporation. I received a master of science in mechanical engineering from the University of California at Berkeley and a bachelor of science in engineering from Swarthmore College.

Symantec protects much of the world's information, and is the largest security software company in the world, with 33 years of experience developing Internet security technology and helping consumers, businesses and governments secure and manage their information and identities. Our products and services protect people's information and their privacy across platforms – from the smallest mobile device, to the enterprise data center, to cloud-based systems. We have established some of the most comprehensive sources of Internet threat data in the world through our Global Intelligence Network, which is comprised of hundreds of millions of attack sensors recording thousands of events per second, and more than 500 dedicated security engineers and analysts. We maintain nine Security Response Centers and six Security Operations Centers around the globe. Every day we scan 30 percent of the world's enterprise email traffic, and process more than 1.8 billion web requests. All of these resources combined allow us to capture worldwide security data that give our analysts a unique view of the entire Internet threat landscape.

The focus of today's hearing is right on point: cybersecurity is a shared responsibility and the public and private sectors must work together closely to counter ever-evolving threats. I am excited to share my and Symantec's expertise to assist the government in improving its cybersecurity posture. In my testimony today, I will discuss:

- The current threat environment;
- An overview of how large organizations can protect themselves; and
- How we partner with the government to improve cybersecurity.

I. The Current Cyber Threat Landscape

Many of the recent headlines about cyber attacks have focused on data breaches in government and across the spectrum of industries. Indeed, the recent theft of personally identifiable information (PII) is unprecedented – over just the past three years alone, the number of identities exposed through breaches surpassed *one billion*. Yet while the focus on data breaches and the identities put at risk is certainly warranted, we also must not lose sight of the other types of cyber attacks that are equally concerning and can have damaging consequences. There are a wide set of tools available to the cyber attacker, and the incidents we see today range from basic confidence schemes to massive denial of service attacks to sophisticated (and potentially destructive) intrusions into critical infrastructure systems. The economic impact can be immediate with the theft of money, or more long term and structural, such as through the theft of intellectual property. It can ruin a company or individual's reputation or finances, and it can impact citizens' trust in the Internet and their government.

The attackers run the gamut and include highly organized criminal enterprises, disgruntled employees, individual cybercriminals, so-called "hacktivists," and state-sponsored groups. The motivations vary –

the criminals generally are looking for some type of financial gain, the hacktivists are seeking to promote or advance some cause, and the state actors can be engaged in espionage (traditional spycraft or economic) or infiltrating critical infrastructure systems. These lines, however, are not set in stone, as criminals and even state actors might pose as hacktivists, and criminals often offer their skills to the highest bidder. Attribution has always been difficult in cyberspace, and is further complicated by the ability of cyber actors to mask their motives and objectives through misdirection and obfuscation.

Attack methods vary, and the only constant is that the techniques are always evolving and improving. Spear phishing, or customized, targeted emails containing malware or malicious links, is the most common form of attack. Many of these attacks are extremely well-crafted; in the case of one major attack, the spear phishing email was so convincing that even though the victim's system automatically routed it to junk mail, he retrieved it and opened it – and exposed his company to a major breach.

In addition, the attack surface continues to expand as both the private and public sectors move to the cloud. Cloud security creates new types of challenges as information is now hyper-distributed -- even tracking where your information is located is a significant problem for most large organizations. Further, the Internet of Things, or IoT, and the billions of new devices coming online, many of which create sensitive information, are posing the next generation of security challenges. And of course there are many IoT use cases that touch critical infrastructure, including transportation, smart buildings, smart cities, smart energy, etc.

Social media is an increasingly valuable tool as people tend to trust links and postings that appear to come from a friend's social media feed and rarely stop to ask if that feed may have been compromised or spoofed. We have also seen the rapid growth of targeted web-based attacks, known as "watering hole" attacks. Like the lion in the wild who stalks a watering hole for unsuspecting prey, cybercriminals lie in wait on legitimate websites that they previously compromised and use to infect visitors. Most of these attacks rely on social engineering – simply put, trying to trick people into doing something that they would never do if fully cognizant of their actions. For this reason, we often say that the most successful attacks are as much psychology as they are technology.

And while many assume that these attacks are the result of sophisticated malware or a well-resourced state actor, the reality is much more troubling. According to a 2015 report from the Online Trust Alliance, 90 percent of the breaches in 2014 could have been prevented if organizations implemented basic cybersecurity best practices.[1] Unfortunately, systems of all types – from the home computer to those running our nation's critical infrastructure – are similarly vulnerable. The good news is that most of these attacks can be stopped, or at worst contained, if organizations use modern security tools and best practices.

II. A Unified Approach to Security

Good security is layered security, and it requires unity of effort. At Symantec, we refer to this as our *Unified Security Strategy*. An organization cannot just throw technology or money at the problem haphazardly and hope for the best. Nor can organizations expect to remain outside the fray – attackers will find and target them, and in all likelihood will find some vulnerabilities to try to exploit. To counter this, organizations need to plan – to defend their systems, to protect their most critical data, and to respond and recover when they are attacked. It is important to recognize that the compromise of one computer or system is not the end of the story, but rather just the beginning. The efficacy of the

[1] https://www.otalliance.org/news-events/press-releases/ota-determines-over-90-data-breaches-2014-could-have-been-prevented

security tools installed and the quality of the plans put in place are the key factors that will determine how successful an organization will be in thwarting an attacker.

The National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Security (also known as the Cybersecurity Framework or CSF), is an excellent tool for organizations of all sizes.[2] NIST worked closely with the private sector for more than a year to develop the CSF, and the result is a document that reflects the best thinking of cyber experts from across the spectrum of security vendors and industry users. The CSF is not your traditional government document – it is not a standard, a set of controls, or a checklist. Instead, it is a tool to help organizations assess and improve their cybersecurity programs, or to build one if they do not already have one. The CSF "core" consists of five functions:

- **Identify** – understand what systems, assets, data, and capabilities need to be protected and establish processes to do so;
- **Protect** – develop and implement appropriate safeguards to critical services;
- **Detect** – develop and implement the appropriate activities to identify a cybersecurity event;
- **Respond** – develop and implement the ability to respond to a cybersecurity event; and
- **Recover** – develop the ability to restore capabilities if they are impaired by a cybersecurity event.

The CSF breaks each core function into "Categories" and then further into "Subcategories," and for each Subcategory, NIST provides a list of existing, commonly-accepted standards or practices that illustrate a method for accomplishing the designated activity. A category is a set of cybersecurity activities under a designated core function, and subcategories are tactical activities that are supposed to satisfy the programmatic needs of a given category.

Notably, the CSF is as useful for more traditional business functions as it is for security professionals; in fact, at Symantec we used the core functions of the CSF to brief our Board of Directors on our internal security posture while the CSF was still in draft form. Late last year, NIST issued a Request for Information seeking feedback on whether the CSF should be updated, and we look forward to working with NIST to evolve the CSF further.

This unified approach to security will benefit the government just as much as it will the private sector, and there are numerous private sector best practices and standards (many of which are included in the CSF) that could improve the cybersecurity of Federal agencies. So too will full implementation of cutting edge security tools, many of which are already owned by the Federal government. The government has made strides over the past few years to improve its cybersecurity posture, and the renewed focus after the OPM breach has accelerated needed improvements. It is clear that modernizing any organization's security posture, whether it be government or industry, is not a unique endeavor. As such, the government should look to those organizations with strong lessons learned, and the experts who aided them, for assistance in securing their networks.

Digging Deeper – How Organizations can Protect Themselves

Many organizations manage their own security, but even some of the country's largest companies have looked to outside experts to assist with their security programs or even to run them. For those who look for outside support, there are a several providers who can assist them, and we offer a wide range of support through our *Managed Security Services* unit. Organizations can bring in experts for everything

[2] http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

from backstopping their own security programs to managing their complete day-to-day operations. But irrespective of whether an organization manages its own security or engages outside experts, the CSF provides a structure for a holistic approach to cybersecurity, and the five core functions serve as an outline for discussing a unified approach to security.

Identify – Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.[3]

Simply put, one cannot effectively protect what cannot be seen – this is the foundation for all security planning. But the task goes beyond just identifying hardware and software – it includes the planning that will carry throughout a security program. This is where organizations put policies in place to ensure that assets are identified and protected, to know what to do when policies are violated, and to be prepared to respond to an intrusion.

The identification has to be flexible, and a good plan will recognize that in a large enterprise it is impossible to have 100 percent awareness of every asset 100 percent of the time. Thus, the security plan and related policies need to account for this reality. The organization must have tools to assess risk and to remediate it, based on the severity. It is important to use a risk-based approach as not all assets are created equal, and not all data carries the same value. Thus, you have to put your security investments against the things that matter the most.

To accomplish these functions, there are technological solutions that can scan networks to map systems and find assets. At Symantec, we provide a tool called *IT Management Suite (ITMS)* which performs hardware and software asset discovery and management. We also have a tool known as *Control Compliance Suite (CCS)* that has a standards management module that allows an organization to conduct scans to determine whether assets are appropriately configured. CCS also contains a policy manager tool that provides an easy way to establish and update company-wide policies as well as to check compliance with those policies.

Protect – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services. [4]

There are numerous elements to this function, both human and technological. On the human side, an organization needs to ensure that its workforce practices good cyber hygiene, is alert for the latest scams and schemes, and understands the security policies. This is a continuing process – new staff needs to be trained, and existing employees need refreshers and updated training. An alert employee can prevent an intrusion or, if a system is already compromised, spot anomalous behavior that could allow a compromise to be contained before any damage is done.

For example, at Symantec we regularly send phishing emails to our own employees both to keep them sharp and to educate them about new and evolving phishing techniques. Individuals who are fooled by the phishing attempts are provided with a short on-line tool that educates them on how to spot them in the future. This program, known as *Symantec Phishing Readiness*, is available for our customers to use so that they too can provide training and awareness in real time.

Unfortunately, not all breaches happen because of accidental or inadvertent actions – malicious insiders pose a real and significant threat. Here technology can help, as strong identity and access management

---

[3] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014 at p. 8 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

[4] *Id.*

tools are key to preventing harm by malicious insiders. These tools can do more than limit data access to users with a need to know – they can do social mapping which will learn how users behave on networks and then alert managers to any unusual or outlying activity. These tools can verify that a user is who they claim to be, and that they have the correct credentials to access the system or particular data. At Symantec, we employ a variety of tools including our own *Validation and ID Protection service (VIP)* and our *Identity Access Manager*.

Identity verification is essential for all users, and user authentication is a core component of our unified security approach. VIP and Identity Access Manager fill that role for us. We are well past the days when a password, even a complex one, will be much more than a speed bump for a sophisticated attacker. Multi-factor authentication – combining something you know (such as a password) with something you have (such as an authentication token or mobile application) – is essential for any system to be secure. Many of the recent high profile breaches would have been prevented had the victims employed multi-factor authentication. A good access manager can also minimize the number of passwords employees need to keep, as it can serve as a portal to myriad tools after the user is properly authenticated.

To combat ever-evolving threats, organizations need to protect both their systems and their data. Perimeter security such as a firewall that scans incoming and outgoing traffic is one piece of the puzzle, but it is just a start. Most intrusions begin on a single compromised device which the attacker uses to establish a beachhead. To counter this, modern endpoint security will do two things that go far beyond the simple antivirus of the past. First, it will look at the age, frequency, location and other characteristics of any file that tries to execute on a computer to expose unknown or emerging threats that might otherwise be missed. For example, if a computer is trying to execute a file that the security system has never seen anywhere in the world and that comes from an unknown source, there is a high probability that it is malicious. Second, it will monitor the overall operation of the system to look for unusual, unexpected, or anomalous activity that could signal an infection. At Symantec, we refer to this as reputation-based security that looks holistically at numerous factors associated with digital files to determine how safe it may be on the security spectrum. We do this through tools such as *Symantec Endpoint Protection* and *Data Center Security*.

Data protection is equally important, and a comprehensive security plan tackles data protection with tools that are distinct from those designed to prevent intrusions. A good data loss prevention (DLP) system will index, track, and control the access to and movement of even huge volumes of data across an organization, and most importantly will prevent data from moving outside an organization. Organizations also should use encryption technology on particularly sensitive data, which renders it unreadable to anyone who does not have the specific cryptologic key. Finally, as part of a risk based approach, after identifying the most valuable data – the so-called "crown jewels" – one needs to apply appropriate protections, which can include virtually or physically isolating a system, applying additional access controls to it, and more. Symantec is a provider of *Endpoint Encryption*, as well as *Data Loss Prevention (DLP)* software, which is an industry leading tool that allows organizations to tailor these controls to their specific needs.

Organizations should also look at any characteristics peculiar to their operation and determine if there are additional protections available that will make it harder for an attacker. For example, in the retail world, there are tools that can be applied to point of sale systems that will virtually lock down the system and only allow it to perform those limited functions that are absolutely necessary for completing a sales transaction. Symantec's *Critical System Protection (CSP)* is highly effective at preventing the theft of credit card and other personal information from these systems because it does not allow unknown or malicious code to execute on the device. In the critical infrastructure sectors, CSP can assist operators to ensure that the systems that control machinery and other critical systems are hardened and isolated to prevent an attacker from being able to reach them, even if the organization's business systems were compromised.

Detect – Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. [5]

In the simplest of terms, an organization needs to know what is going on inside of its systems – as well as who is trying to access it and how they are trying to do so. Good security means looking for anomalous behavior that could indicate the presence of a new threat or a previously unknown attack. Modern security suites will look at the connections that your system is making to see if a machine is talking to a known bad actor or to a suspicious domain; they will look for activity that is outside the normal behavior for a given machine; and they will flag unusual transfers of data, whether within a system or to someone outside of it. But detection goes beyond monitoring what the machines are doing – it is equally important to assess authorized user activity to look for both accidental and intentional violations of security policies. This can include transferring a business file to a personal device to work on at home or a large scale theft of company data.

Analytics such as these are perhaps the fastest evolving area in cybersecurity. Modern security suites ingest a huge volume of machine and user data and, using rules set by the organization, develop a profile of what is normal and allowed for a given system or user. These systems learn continuously, and alert when a rule or policy is violated. The key to doing this effectively is identifying what to look for – a system is only as smart as the rules that govern it and the data it has to analyze. The latest evolution in this approach is systems that draw inferences from seemingly unconnected bits of data and, using advanced behavioral and reputation analytics, know that a series of anomalies could be an indicator of malicious activity. By doing so, these systems are able to detect threats that bypass other protections.

At Symantec, we refer to this as our *Unified Security Analytics Platform*. It derives information from Symantec protected endpoints, data centers, and gateways and incorporates log and telemetry files, behavioral, reputation, and threat analytics, global threat intelligence, and actionable insights to provide the key inferences to connect the dots. We use this to protect our own networks and those of our customers worldwide.

Respond – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. [6]

Good planning is the foundation of an effective response, and studies have shown that organizations that prepare in advance minimize the damage of a breach and expend fewer resources when an incident occurs. [7] Planning is both a human and a machine exercise. It is up to an organization's leaders to stress the importance of preparation and to lead the effort, and key responders need to be identified and trained ahead of time. Indeed, everyone involved in the response should know his or her roles and responsibilities before an event happens.

It is also useful to identify ahead of time any outside expertise that may be needed to contain a major incident. Interviewing potential responders is not a good use of an organization's time while it is hemorrhaging sensitive data, and the middle of a crisis is rarely the best time to make decisions about outside vendors. It also is useful to establish relationships with law enforcement before an attack so that you know who to call should an incident occur. Hours spent determining who is the appropriate agency to contact could be additional hours that an attacker is on your system. Moreover, should an incident escalate to the point that law enforcement is involved, it will likely be necessary to take steps to preserve log files and other data as forensic evidence – and pre-planning will help to ensure that this

---

5 *Id.*

6 *Id.*

7 2015 Cost of Data Breach Study: A Global Analysis, Ponemon Institute LLC, May 2015 at p. 13 (http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03053wwen/SEW03053WWEN.PDF?)

happens effectively. At Symantec, we have a unit called *Cyber Security Services* that can help organizations prepare for and respond to breaches.

A good planning process will necessarily lead to implementation of better security practices and tools – and will streamline the response process and limit the damage an organization will suffer. Finally, a plan needs to be exercised, both to train employees and to identify areas for improvement. At Symantec, we conduct simulation exercises (our internal "Cyber War Games") that provide hands-on training for our employees. This proved to be such a success that we developed a commercial version of it, and offer *Security Simulations* that our customers can use to train their own employees. These simulations provide a controlled environment for defenders to think like the bad guy – which in turn makes them better at protecting their systems.

Recover – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event. [8]

Recovery is two-fold – getting the impacted systems back up and running, and improving security based on the lessons learned from the incident. Resilience in both systems and data is essential; an organization needs clean computers and clean back-ups as recovering from a major incident will frequently involve taking systems offline, reimaging them, and restoring data. Thus, effective and efficient recovery requires preparation and planning. Making decisions and hiring vendors or consultants on the fly after an incident will certainly increase the time to get back up and very likely raise the cost of doing so. And poor preparation could leave an organization with incomplete or corrupted backups, making recovery all the more difficult.

But perhaps the hardest part is ensuring that an organization has an effective feedback loop – the ability to fix identified flaws in both systems and processes. Much of this will happen after an incident is resolved, and too often organizations are either too busy getting back up to speed or too exhausted from the event to do a thorough after-action review. Nevertheless, the immediate aftermath of the event is the best time to implement security improvements, update response plans, and consider new policies and procedures.

For example, our Global Security Office, led by our Chief Information Security Officer who is responsible for Symantec's cyber and physical corporate security, has a planning team dedicated solely to responding and recovering. They manage the planning process and any feedback loops for improvement. This plan is integrated to include all components of the response and recovery effort, including products, technology response, sales, legal, public relations, and more. The plan is reviewed regularly with the components and exercised throughout the year.

III. Partnering with the Government to Improve Cybersecurity

Symantec views our role in combating global cyber threats as a core value for the company. As such, we participate in numerous industry consortia, as well as public-private partnerships with all levels of government, both here in the U.S. and abroad. We share high-level cybercrime and cyber threat trends and information on a voluntary basis through different fora to help protect our customers and their networks. Effective sharing of actionable information among the private sector, and between the public and private sectors, on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity and deterring cybercrime. Of course, all of this work is done in keeping with both our strict privacy policies, and all applicable privacy and data protection laws.

[8] Framework for Improving Critical Infrastructure Cybersecurity, National Institute of Standards and Technology, February 12, 2014 at p. 8 (http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf).

Among the public-private partnerships Symantec participates in are the National Cyber-Forensics and Training Alliance (NCFTA), FBI, EUROPOL, INTERPOL, the North Atlantic Treaty Organization (NATO), and AMERIPOL. The NCFTA demonstrates how private industry and law enforcement partnerships can yield real world success. Based in Pittsburgh, the NCFTA includes more than 80 industry partners – from financial services and telecommunications to manufacturing and health care – working with federal and international partners to provide real-time cyber threat intelligence to identify threats and actors. In turn, the NCFTA provides intelligence to domestic and international law enforcement to counter those threats. Through this partnership, hundreds of criminal investigations have been launched, which otherwise would not have been addressed, with successful prosecutions of more than 300 cyber criminals worldwide. In further support of these initiatives, the NCFTA has produced more than 400 cyber threat intelligence reports over the past three years alone. Through the NCFTA, industry is able to share crucial cyber threat information across a broad group of private industry and law enforcement entities at home and abroad. [9]

Symantec also maintains relationships in the U.S. and around the world with international cyber response organizations and law enforcement entities including the FBI, INTERPOL, EUROPOL, and dozens of national Computer Emergency Response Teams (CERTs) and police forces, by sharing the latest technological trends, the evolution of the threat landscape, and the techniques that cyber criminals use to launch attacks.

For example, in June of 2014, Symantec, the FBI, and a number of international law enforcement agencies mounted a major operation against the financial fraud botnet *Gameover Zeus* and the ransomware network *Cryptolocker*. *Gameover Zeus* was the largest financial fraud botnet in operation that year and is often described as one of the most technically sophisticated variants of the ubiquitous *Zeus* malware. Symantec provided technical insights into the operation and impact of both *Gameover Zeus* and *Cryptolocker*, and worked with a broad industry coalition and the FBI during this case. As a result, authorities were able to seize a large portion of the infrastructure used by the cybercriminals behind both threats.[10]

In February of 2015, Symantec and other industry players partnered with EUROPOL in an operation against the *Ramnit* botnet and seized its servers and infrastructure. *Ramnit* harvested banking credentials and other personal credentials from their victims. The group was in operation for at least five years and had evolved into a major criminal operation, infecting more than 3.2 million computers.[11]

Symantec also works closely with INTERPOL. In November of 2015, Symantec was invited to present at INTERPOL's Africa Cybercrime Working Group meeting held in Kigali, Rwanda. The event provided a rare forum for law enforcement cybercrime units from 13 African countries and several industry partners to exchange threat information and discuss cross-border cybercrime challenges in Africa.

In December of 2015, Symantec signed a partnership agreement with NATO's Communications and Information (NCI) Agency. NATO recognizes the importance of working with industry to address emerging cybersecurity challenges that may affect the ability of NATO to achieve its mission of defending its member nations. A number of activities are already underway, including sharing cyber threat information, capacity building and promoting technological innovation to address emerging challenges.[12]

[9] https://www.ncfta.net/about-ncfta.aspx
[10] http://www.symantec.com/connect/blogs/international-takedown-wounds-gameover-zeus-cybercrime-network
[11] http://www.symantec.com/connect/blogs/ramnit-cybercrime-group-hit-major-law-enforcement-operation
[12] https://www.ncia.nato.int/NewsRoom/Pages/151211_NATO-builds-cyber-alliances.aspx

Symantec also has partnered with AMERIPOL and the Organization of American States to publish a report in June of 2014 that provided the most comprehensive snapshot to date of cybersecurity threats in the Latin American and Caribbean region. The goal was to raise awareness of cybercrime issues and promote the importance of cybersecurity throughout the region as national and economic security imperatives. Similarly, Symantec is partnering with the African Union and the United States Department of State Office of the Cyber Coordinator to develop a report examining the cybersecurity threats and trends in Africa. That report will be published later this year.

Private to private partnerships have also proven to be effective in fighting cybercrime. An excellent example of the private sector banding together is the establishment of the Cyber Threat Alliance (CTA). The CTA is a group of cyber security practitioners from Symantec, Intel Security, Palo Alto Networks and other firms that have chosen to work together in good faith to share threat information for the purpose of improving defenses against advanced cyber adversaries across member companies and their customers. By sharing detailed security information we can improve overall protection for our customers – many of whom use multiple security products. The bulk of information sharing before the CTA was established primarily involved sharing malware samples. The CTA builds upon this foundation by sharing more actionable threat intelligence, including information on zero day vulnerabilities, botnet command and control server information, mobile threats, and indicators of compromise related to advanced persistent threats, to combat more advanced attacks. [13]

Conclusion

Cybersecurity is not the sole province of the government or the private sector; the only path to improving security for the Nation is through partnership and shared expertise. The NIST CSF – itself the result of a successful collaborative public-private effort – is a tool that can be used to build out a cybersecurity program or to assess an existing one. It is equally useful to Federal agencies, which can use it to assess their own security posture as well as look to private sector experience with the CSF in order to maximize its utility. Similarly, the government can look to the private sector's experience incorporating cutting edge security tools into their security programs. Simply put, good standards and policies in combination with tools like data loss prevention, endpoint security, strong firewalls, security analytics, and multi-factor authentication are the building blocks of a good cybersecurity program.

We appreciate the Committees' interest in learning from Symantec's expertise and best practices, and we look forward to continuing to partner in the future.

[13] http://cyberthreatalliance.org/mission.html