Prepared Testimony and
Statement for the Record of

Cheri F. McGuire
Vice President, Global Government Affairs & Cybersecurity Policy
Symantec Corporation

Hearing on

"Striking the Right Balance:
Protecting Our Nation's Critical Infrastructure from
Cyber Attack and Ensuring Privacy and Civil Liberties"

Before the

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure
Protection and Security Technologies

April 25, 2013

311 Cannon House Office Building

Chairman Meehan, Ranking Member Clarke, and distinguished members of the Subcommittee, thank you for the opportunity to testify today on behalf of Symantec Corporation.

My name is Cheri McGuire and I am the Vice President for Global Government Affairs and Cybersecurity Policy at Symantec. I am responsible for Symantec's global public policy agenda, including cybersecurity, data integrity, critical infrastructure protection (CIP), and privacy. In this capacity, I work extensively with industry and government organizations, including serving from 2010 to 2012 as Chair of the Information Technology Sector Coordinating Council (IT SCC) – one of 16 critical sectors identified by the President and the US Department of Homeland Security (DHS) to partner with the government on CIP and cybersecurity. I also serve as a board member of the Information Technology Industry Council, the TechAmerica Commercial Policy Board, and the US Information Technology Office (USITO) in China, and am a past board member of the IT Information Sharing and Analysis Center (IT-ISAC). Prior to joining Symantec in August 2010, I was Director for Critical Infrastructure and Cybersecurity in Microsoft's Trustworthy Computing Group. Before joining Microsoft in 2008, I served in numerous positions at DHS, including as Acting Director and Deputy Director of the National Cyber Security Division and US Computer Emergency Readiness Team (US-CERT).

Symantec is the largest security software company in the world, with over 31 years of experience in developing Internet security technology. We are the global leader in providing security, storage and systems management solutions to help consumers and organizations secure and manage their information and identities. We protect more people and businesses from more online threats than anyone in the world. Symantec has developed some of the most comprehensive sources of Internet threat data through our Global Intelligence Network (GIN). Comprised of approximately 69 million attack sensors, the GIN records thousands of events per second and covers over 200 countries and territories 24 hours a day, seven days a week. It allows us to capture worldwide security intelligence data that gives our analysts an unparalleled view of the entire Internet threat landscape, including emerging cyber attack trends, malicious code activity, phishing and spam.

Symantec also maintains one of the world's most comprehensive vulnerability databases, currently consisting of more than 51,000 recorded vulnerabilities (spanning more than two decades) from over 16,000 vendors representing over 43,000 products. Every day we process more than three billion e-mail messages and more than 1.4 billion web requests across our 14 global data centers. In short, if there is a class of threat on the Internet, Symantec knows about it.

At Symantec, we are committed to assuring the privacy, security, availability, and integrity of our customers' information. Too often security is portrayed as being in conflict with or somehow undermining privacy. In the digital world, nothing could be further from the truth, because your privacy is only as secure as your data.

We welcome the opportunity to provide comments as the Committee continues its important efforts to bolster the state of cybersecurity while protecting privacy in the US and abroad. In my testimony today, I will provide the Subcommittee with:

- our latest analysis of the threat landscape as detailed in the just-released Symantec Internet Security Threat Report (ISTR), Volume 18;
- our core privacy principles;
- an overview of the current information sharing environment; and
- a summary of how we ensure privacy when we share threat information.

Today's Threat Landscape

We rely on technology for virtually every aspect of our lives, from driving to and from work, to mobile banking, to securing our most critical systems. As the use of technology increases so do the volume and sophistication of the threats. At Symantec, it is our goal to ensure that we are thinking ahead of the attackers. Looking at the current threat landscape is not enough – we must also keep our eyes on the horizon for evolving trends.

In the latest Symantec Internet Security Threat Report (ISTR), we detail that in 2012, approximately 93 million identities were exposed through hacking, theft, and simple error. That is 93 million individuals whose personal information is now potentially for sale in the black market – 93 million people who are at risk for credit card fraud, identity theft, and other illegal schemes.

We also found that there was a 42 percent rise in targeted attacks last year.[1] It is almost certain that this trend will continue in the coming years. Conducting successful targeted attacks requires attackers to do research about the organizations they are seeking to penetrate, and often about specific people who work there. Attackers will mine the Internet for information about how a company does business and use what they learn to craft personalized attacks designed to gain access to its systems. Once they gain access, they will move within a system, collecting information and staging data for exfiltration – the unauthorized transfer or release of data from a computer or server – to their own computers. Attackers can spend weeks and months covertly moving around a victim's system, collecting e-mail, personal data, documents, intellectual property, and even trade secrets.

We also saw a sharp rise in the exploitation of mobile malware. Last year, mobile malware increased by 58 percent, and 32 percent of all mobile threats attempted to steal personal information, such as e-mail addresses and phone numbers. Attacks on mobile devices will almost certainly continue to rise as we become ever more reliant on these devices to perform our daily activities, such as working, banking, shopping, and social networking.

Another alarming finding was the rise of attacks on small and medium size businesses. In 2012, 50 percent of all targeted attacks were aimed at businesses with fewer than 2,500 employees, and the largest growth area for targeted attacks was aimed at businesses with fewer than 250 employees. Thirty-one percent of all attacks targeted them, up from 18 percent the year before. This likely stems from the fact that unlike large enterprises, smaller businesses often do not have the resources to install adequate security protocols, making them an easier target for

[1] *Symantec Internet Security Threat Report* XVIII, April 2013.
http://www.symantec.com/security_response/publications/threatreport.jsp

attackers. Yet many of these small companies subcontract or work for larger companies – and thus hold intellectual property and trade secrets coveted by attackers. As one of our security engineers likes to say, while every subcontractor may sign a strict non-disclosure agreement, the attacker who is sitting on that small company's system is not bound by it.

In sum, whether they are attacking our computers, mobile phones or social networks, cyber-criminals are looking to profit by spying on us or stealing our information. Our best defense is strong security, education, and good computer hygiene.

Privacy and Security Go Hand in Hand

At Symantec, we are guided by the following privacy principles: First, customers should be empowered to decide how their personal information is used, and informed what – if anything – will be done with it. Second, privacy protections must be integrated into the development of products or services and not added as an afterthought. Finally, we all need to be proactive in protecting privacy – absent strong security, information is vulnerable.

Criminals and hackers – many of whom are well-funded and highly skilled – have built a business model based on their ability to steal and monetize personal information. There is an entire criminal eco-system that trades in stolen personal information, as well as the tools and technology that allow them to steal more. Some of these criminal enterprises are so sophisticated that they provide 24/7 customer support, and offer guarantees that the stolen information they provide is valid.

In the face of this criminal threat, it should go without saying that strong security is essential to securing our personal data and private information. Simply put, if your data is not secure, then neither is your privacy. And, if you do not take steps to secure your own personal information, or the companies to which you entrust it do not do so, you are gambling with your privacy. When it comes to personal data, security measures and data protection are not an infringement on privacy but instead are the foundations of protecting it.

Recent efforts to improve the Nation's cybersecurity posture – whether legislative initiatives or executive branch actions – have recognized that privacy and security must be addressed in tandem. The various bills in the House and the Senate have taken different approaches, but in the information sharing area there is broad agreement that both the government and the private sector need to be able to share cybersecurity information for cybersecurity purposes. This view also is shared by many prominent civil society organizations. Reaching consensus on the precise parameters of those terms is where complications have arisen. Symantec supports an approach that allows us to share threat indicators and related non-Personally Identifiable Information (PII) within industry and with the government. In our view, companies should receive legal protection for sharing appropriate information with other companies or civilian agencies, and we believe that data minimization standards are a reasonable approach.

The Current Information Sharing Environment

Globally, there are many different information sharing models, ranging from voluntary programs to regulatory mandates to *ad hoc* arrangements to contractual agreements. Sharing can be government to government, business to business, and between government and business. As a general rule, we believe that voluntary programs – which of course leave space for contractual and *ad hoc* arrangements – are the best way to develop trusted partnerships to achieve the best results. In the U.S., we have a voluntary framework based on the National Infrastructure Protection Plan (NIPP).[2] The NIPP, as refined by the recent Presidential Decision Directive 21, establishes 16 critical infrastructure sectors and identifies a sector-specific federal agency for each. [3]

Within each sector, there are Government Coordinating Councils (GCC) and Sector Coordinating Councils (SCC). Nearly all sectors also have chartered Information Sharing and Analysis Centers (ISAC), operational entities that are tied to industry and serve as a focal point for voluntary information sharing. The level of trusted partnership and engagement among the GCCs, SCCs and ISACs varies from sector to sector. Symantec has a long and successful history of participation and leadership in various multi-industry organizations as well as public-private partnerships in the US and globally, including the National Cyber-Forensics & Training Alliance (NCFTA), the IT-ISAC, the Industry Botnet Group Mitigation Initiative, and many others.

Effective sharing of actionable information among the public and private sectors on cyber threats, vulnerabilities, and incidents is an essential component of improving cybersecurity. It is important to recognize that information sharing is not an end goal, but rather is one of a number of tools to enhance the security of IT systems. Good information sharing provides situational awareness so that appropriate protective and risk mitigation actions can be put into place. In order for information sharing to be effective, information must be shared in a timely manner, must be shared with the right people or civilian organizations, and must be shared with the understanding that so long as an entity shares information in good faith, it will not face legal liability.

The NCFTA provides a good example of how private industry and law enforcement partnerships can yield real world success. NCTFA is a Pittsburgh-based organization that includes more than 80 industry partners – from financial services and telecommunications to manufacturing and others – working with federal and international partners to provide real-time cyber threat intelligence.

The IT-ISAC is another example of a successful public-private partnership. The group's primary purpose is to allow organizations to exchange information about security threats and vulnerabilities. Member companies report information concerning security problems that they

[2] National Infrastructure Protection Plan (2009), http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[3] The 2009 National Infrastructure Protection Plan (http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf) identified 18 critical infrastructure sectors. Presidential Decision Directive 21 (Critical Infrastructure Security and Resilience, signed February 12, 2013) revised that to 16. *See* http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

have or solutions to such problems that they have found. Members also participate in national and homeland security efforts to strengthen IT infrastructure through cyber threat information sharing and analysis. The IT-ISAC also has an industry-funded representative that works at the National Cybersecurity & Communications Integration Center (NCCIC) to facilitate real-time information sharing and response.

One of the most successful US public-private partnerships has been cybersecurity exercises. The level of engagement and resources brought to bear from the government and industry to jointly plan and develop scenarios, define information sharing processes, and execute the exercises has been unprecedented. When done right, the lessons learned from these exercises have been invaluable to both industry and government to help improve response plans and improve preparedness for future incidents.

In addition, the government must have the proper tools and authorities to disseminate information effectively. I have seen too many instances of the government releasing information on cyber threats days and sometimes weeks after a threat has been identified. In many of these cases, by the time the government releases the information it often has little use because the private sector has already identified and taken actions to mitigate the threat. There is no single solution that will eliminate these delays, but various legislative proposals move us one step closer to eliminating some of the legal barriers that currently impede sharing. Moreover, the Executive Order (EO) the President signed in February 2013 sent a clear message to the government that sharing information with the private sector is both a priority and a necessity.[4]

Further, we also support an incentive-based approach to information sharing. There is no doubt that businesses can gain a competitive advantage by not disclosing information to their competitors. However, a well-incentivized program of collaboration can help offset those disadvantages and keep the information flowing freely. We also need to address policies that discourage businesses who would be willing to share information but choose not to because of fear of prosecution. Therefore, liability protections are necessary to improve bi-directional information sharing.

As with any partnership, information sharing is founded upon and enabled by trust. That trust is weakened when government information sharing mandates are imposed on industry. Enhanced self-interest and a flexible approach are more likely to improve information sharing than government mandates.

Protecting Privacy as We Share Threat Information

At Symantec, we understand the vital importance of sharing information for cybersecurity awareness and response. We recognize that information stored on our servers is sensitive, confidential and often personal in nature. Therefore, we take very seriously our role in safeguarding our customer's personal information and go to great lengths to ensure that personal information remains private.

[4] *See* Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11739 (February 19, 2013).

Information pertaining to customers such as credit card information, addresses or other PII is not shared under any circumstances unless we are compelled by law, following appropriate due process. In addition, we comply with the Payment Card Industry Data Security Standard and follow specific rules under our privacy program to ensure that we collect only data that is proportionate for the purposes for which it is collected, and that is relevant and necessary for the services provided.

Information sharing on cyber threats happens in a number of ways and for various reasons. We get information from myriad sources – from our customers, our partners, the government, and our network of sensors. The information itself can be high-level threat data, details about a particular incident or attack, data signatures, or other information. All of this data is then aggregated and analyzed, and during that process we remove PII. The resulting work product can range from machine-level signatures or identifying information for a specific piece of malware to a quick analysis of a particular attack to a published white paper on current and future threat vectors. This work product can then be provided to our customers and partners in both the private sector and the government, depending on the particular parameters of the sharing agreement.

In some cases, the communication is purely bilateral – a customer provides us information about activity on its system (either manually or through an automated sensor), and we report back on what we see happening. Other times we share it broadly, including sometimes publicly, but only after removing any PII to ensure that the report cannot be linked to a particular individual or customer. When we share reports on attack trends or publish white papers on particular threats, PII is removed as part of long-standing policy and we only share information directly related to the cyber threat. We have legal and organizational safeguards to ensure that information is only disclosed to the intended partners and only used for the expressed purpose.

In closing, Symantec is deeply committed to securing the privacy and security of our customer's information. Thank you again for the opportunity to testify, and I will be happy to answer any questions you may have.