STATEMENT OF PHYLLIS SCHNECK

VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

MCAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

HOMELAND SECURITY COMMITTEE

SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND SECURITY TECHNOLOGIES

"EXAMINING THE CYBER THREAT TO CRITICAL INFRASTRUCTURE AND THE AMERICAN ECONOMY"

MARCH 16, 2011

Chairman Lungren, Ranking Member Clarke, and other distinguished members of the Subcommittee, thank you for requesting McAfee's views on the cyber threat to critical infrastructure and the American economy. Your committee is playing a vital role in helping to define the contours of the cyber security debate, and your aim to write thoughtful, incentives-based legislation must be commended.

My name is Phyllis Schneck and I have dedicated my entire professional career to the security and infrastructure protection community. My technical background is in high performance computing and cryptography. In addition to serving as Vice President and Chief Technology Officer, Global Public Sector, for McAfee, I serve as Chairman of the Board of Directors of the National Cyber Forensics and Training Alliance, a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 150 cyber criminals worldwide. Earlier, I worked as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence. I have also served as a

commissioner and working group co-chair on the public-private partnership for the CSIS Commission to Advise the 44th President on Cyber Security.

Additionally, I served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program and as founding president of InfraGard Atlanta, growing the InfraGard program from 2000 to over 33,000 members nationwide. Before joining McAfee, I was Vice President of Research Integration at Secure Computing. I hold a Ph.D. in Computer Science from Georgia Tech, where I pioneered the field of information security and security-based high-performance computing.

My testimony will focus on the following key areas:

- The evolution of the cyber security threat landscape;
- McAfee's Global Threat Intelligence Solution and the role it plays in enabling us to detect and remediate a wide range of cyber security attacks on our nation's critical infrastructures;
- Two major cyber security attacks, Night Dragon and Operation Aurora, and their implications for our homeland security; and
- Policy recommendations to improve public/private sector information sharing that is essential to give the government the capabilities it needs to respond to the modern cyber security challenge.

First I would like to provide a little background on McAfee and some of our cyber security initiatives.

McAfee's Role in Cyber Security

McAfee, Inc. protects businesses, consumers and the public sector from cyber-attacks, viruses, and a wide range of online security threats. Headquartered in Santa Clara, California, and Plano, Texas, McAfee is the world's largest dedicated security technology

company and is a proven force in combating the world's toughest security challenges. McAfee is a wholly owned subsidiary of Intel Corporation.

McAfee delivers proactive and proven solutions, services, and global threat intelligence that help secure systems and networks around the world, allowing users to safely connect to the Internet and browse and shop the web more securely. Fueled by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

To help organizations take full advantage of their security infrastructure, McAfee launched the Security Innovation Alliance, which allows organizations to benefit from the most innovative security technologies from thousands of developers who can now snap into our extensible management platform. Today, more than 100 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Two years ago, McAfee announced an initiative to fight cybercrime, a wide-ranging initiative aimed at closing critical gaps in assisting victims of cybercrime and preventing new events. The initiative is anchored by a multi-point plan that includes calls for action from law enforcement, academia, service providers, government, the security industry and society at large to deliver more effective investigations and prosecutions of cybercrime. Key elements of the plan include:

- Education and Awareness – McAfee works to ensure that officials around the world have the capacity to properly fight cybercrime, while helping users build “street smarts” so that they don’t become easy victims.
- Legal Frameworks and Law Enforcement – McAfee works to facilitate international collaboration and mutual assistance on cybercrime among governments, industry and non-governmental organizations (NGOs).

- Innovation – McAfee works with the technology industry to provide technology solutions that stay one step ahead of the threats.

McAfee is also supportive of the National Strategy for Trusted Identities in Cyberspace (NSTIC), working with our partners in government and industry to enable innovation for more efficient authentication and other technologies facilitating a safer and more pleasant experience for electronic transactions.

McAfee is committed to bringing the best security products and services to the market, partnering with leading IT vendors to ensure that customers have the ability to pick and choose the best solutions to close their security gaps, and giving consumers and organizations additional resources and support to fight cyber-crime ranging from organized financial crime to attacks that user the cyber infrastructure to gain access to intellectual property or physical infrastructure. Likewise, McAfee is committed to taking part in a constructive dialogue with policy makers on cyber security initiatives, as we are pleased to do in this hearing today.

The Evolution of the Cyber Security Threat Landscape

For purposes of this testimony, we define malware as a set of instructions for a computer that causes the computer to behave in the will of the malware owner, such as providing unauthorized access to information or systems that control physical/kinetic infrastructure. Computers execute instructions. Malware puts the enemy's instruction next on the list, and then the adversary controls all actions forward, sometimes hiding its presence. Malware enters a machine from a variety of ports, typically email, web or connection-level access that is unprotected or ill advised to admit these harmful instructions. Malware can also be referred to commonly as a "'virus." As in biology, when a machine has a virus it is compromised and its functions can cause harm.

Historically, security software relied on antivirus "signatures" to recognize and block malware. Once a virus was detected, a signature was developed by the security software

vendor and deployed in the form of a DAT file downloaded to the security software on customers' computers. That software would then be in a position to recognize and block the malware – an approach much like a vaccine that requires advance knowledge of the threat. However, this approach is not sufficiently fast to fight today's cyber adversary, and that is why McAfee is changing the paradigm to proactive defence in real-time: to make our networks sufficiently intelligent to prevent malicious instructions from reaching the target – instead of requiring that the target be vaccinated with a signature.

Today, malware developers combine web, host, and network vulnerabilities with spam, rootkits, spyware, worms and other means of attack. Significantly, malware is often distributed with micro-variations (polymorphism), or the ability to change quickly, with the effect that a signature developed when the malware is first discovered is ineffective against the multiple, very slightly different forms of the same malware. This is analogous to a disease mutating so that the vaccine is no longer effective. Malware may be distributed indirectly by networks of computers that have been corrupted by a criminal (a "botnet").

Criminals, terrorists, and nation states often invest great efforts to deploy their software in hundreds of thousands or indeed millions of computers owned by innocent third parties, in order then remotely to command their botnet to launch an attack on a particular set of targets. The malicious software distributed by botnets will often actively evolve to become whatever is needed by its controller and is not limited by the boundaries of antivirus labels. This means that code that appears otherwise harmless in order to be let into the network can be told to spread rapidly. This is why we refer to this type of code as a worm. It means, for example, that malware originally configured to generate spam messages can be instructed to steal banking information. Again, cyber actions rely on the execution of instructions, and a compromised machine often follows the adversary's instructions to reach out to a server in another location for its next set of instructions, which can vary widely.

By leveraging multiple threat vectors and "one-time usage," hackers are able to extend the time period in which their malware remains undetected and are thus able to steal the

money, personal data, and other valuable information of users throughout the United States and the world. In this way, what might be called classic "viruses" have been blended in recent years with other types of malware and techniques used by malicious hackers intent on stealing personal data. Hackers have discovered that direct external attacks are unnecessary and risky. It is now easier to engineer malicious software that is delivered to a system remotely through various means.

Modern malware thus can no longer be classified by its perceived purpose or propagation method, because those change in an instant. Some types of software can be engineered to gain access to and maintain control over the victim's machine. Once the malware is on the system, it seeks to communicate with its controlling entity – the criminal actor. Once communication is established over the Internet, any compromised machine can be instructed both to pass over any data of value to the criminal and to act as an instrument of attack against other computers and networks.

McAfee Global Threat Intelligence

McAfee and other sophisticated cyber security providers have developed multi-vector, real-time, predictive protection against these more sophisticated attacks on information systems. McAfee's solution is known as Global Threat Intelligence, or GTI. Cyber security solutions based on this GTI approach protect the customer's computer by calculating the potential risk of a piece of content based on experience with the IP address from which it originates, the web site, or other elements associated with the content in question.

Thus cyber security providers offer solutions enabling the customer to stop content that is analyzed as having a risk probability score that in the customer's view is "too risky" to be loaded into the memory of the customer's computer. McAfee GTI tracks the anomalous behavior and proactively adjusts an entity's reputation – its website, IP address, domain, file, network connection, and so forth – so that McAfee products can block the threat and protect customers. Then McAfee GTI looks out across its broad network of sensors and connects the dots between the website and associated malware, email messages, IP

addresses, and other associations, adjusting the reputation of each related entity so that McAfee's security products – from endpoint to network to gateway – can protect users from cyber threats at every angle.

McAfee GTI offers the most comprehensive threat intelligence in the market. With visibility across all threat vectors – file, web, message, and network – and a view into the latest vulnerabilities across the IT industry, McAfee correlates real-world data collected from millions of sensors around the globe and delivers real-time, and often predictive, protection via its security products.

Our cyber enemies are smart and fast. They maintain their knowledge of networks and techniques by freely sharing information, enjoying a lack of legal or intellectual property barriers that often block the defenders. The adversary is well funded, often by governments, and has no barrier to swift execution. This is why our cyber infrastructures have become their play land. The ability to see a global cyber picture and to have situational awareness is what the adversary cannot do. This is where we can win – by making the network fabric reject malicious instructions in real-time, at the speed of light, before they can hit a target. This is how we can be faster than the adversary, and this is the paradigm shift from vaccines to a cyber immune system that enhances cross-sector cyber resiliency.

Our Global Threat Intelligence service as well as a number of our other products and services helped us first detect and then remediate two important global cyber security attacks – Night Dragon and Operation Aurora. These attacks are significant because they were managed by coordinated and organized teams that succeeded in extracting billions of dollars of intellectual property from leading American companies in the information technology, defense and energy sectors – strategic industries vital to the country's long-term economic success and national security.

Operation Aurora

On January 14, 2010 McAfee Labs identified a zero-day (previously publicly unknown) vulnerability in Microsoft Internet Explorer that was used as an entry point for Operation Aurora to exploit Google and at least 20 other companies. Microsoft has since issued a security bulletin and patch.

Operation Aurora was a coordinated attack that included a piece of computer code that exploits the Microsoft Internet Explorer vulnerability to gain access to computer systems. This exploit is then extended to download and activate malware within the systems. The attack, which was initiated surreptitiously when targeted users accessed a malicious web page (likely because they believed it to be reputable), ultimately connected those computer systems to a remote server. That connection was used to steal company intellectual property and, according to Google, additionally gain access to user accounts.

We also discovered that intruders used a social engineering message, known as spear-phishing, to target employees with a high level of access in these companies (either software developers, quality assurance engineers, or domain administrators). The message would come from a previous acquaintance of the targeted user and would ask them to click on a web link pointing to a web server in Taiwan. As we uncovered and then reported to Microsoft, the web link hosted an obfuscated and encoded exploit for a zero-day vulnerability in Internet Explorer.

If a user had clicked on a link with Internet Explorer version 6, their machine would be automatically compromised and malicious code would be downloaded and executed stealthily on the computer. The Trojan would establish an evasive backdoor command and control channel to the same server in Taiwan through which live attackers would jump onto the system and proceed to escalate their privileges on the local machine as well as other servers within the network. As they moved rapidly through the network, they would identify and compromise repositories of intellectual property and exfiltrated data of interest out of the company. In many cases, this data included source code – the crown

jewels of these information technology companies – which then could be used by attackers to discover new vulnerabilities in software that is used by the critical infrastructure industry, government agencies and many other organizations across the globe. McAfee is continuing to work with multiple organizations that were impacted by this attack, as well as with various government agencies, to address this major supply chain attack in the US commercial sector.

Night Dragon

McAfee has identified a string of attacks designed to steal sensitive data from targeted organizations. Unlike opportunistic attacks, the perpetrators appear to be highly organized, premeditative, and motivated in their pursuits.

Night Dragon attacks are similar to Operation Aurora and other advanced persistent threats, or APTs, in that they employ a combination of social engineering and well-coordinated, targeted cyber attacks using remote control software and other malware. McAfee has linked these attacks to intrusions starting in November 2009, and there is circumstantial evidence suggesting they may have begun as early as 2007. Currently, new Night Dragon victims are being identified almost weekly.

Night Dragon attacks leverage coordinated, covert, and targeted cyber attacks involving social engineering, spear-phishing, vulnerability exploits in the Windows operating system, Active Directory compromises, and remote administration tools, or RATs. The attack sequence is as follows:

- Public-facing web servers are compromised via SQL injection; malware and RATs are installed.
- The compromised web servers are used to stage attacks on internal targets.
- Spear-phishing email attacks on mobile, VPN-connected workers are used to gain additional internal access.

- Attackers use password-stealing tools to access other systems – installing RATs and malware as they go.
- Systems belonging to executives are targeted for emails and files, which are captured and extracted by the attackers.

McAfee has evidence of Night Dragon malware infections in the Americas, Europe, and Asia. McAfee has also identified tactics, techniques, and procedures (TTPs) utilized during these continuing attacks that point to individuals in China as the primary source. The Night Dragon attackers are currently targeting global oil, energy, and petrochemical companies with the apparent intent of stealing sensitive information such as operational details, exploration research, and financial data related to new oil and gas field bid negotiations. As we saw with the WikiLeaks document disclosures brought about by a malicious insider, sensitive data theft can be highly damaging beyond regulatory penalties and lost revenue. And unlike Stuxnet, the tools and techniques behind Night Dragon are not specific to critical infrastructure and can be used to launch attacks against any industry.

Policy Recommendations

Officials have made tremendous progress in the creation of information-sharing constructs comprising multiple agencies and the private sector. With good information, the collaboration enabled by these constructs will help us to achieve what the enemy already has: speed and alacrity of information sharing and acting on it for high impact.

In many cases, private sector companies can solve a cyber security puzzle by evaluating many disparate clues. Private companies need protected ways to share their big picture research findings with the government without loss of trust or creation of material events for stockholders, so that the most significant cyber security information is expeditiously actionable. This is the human component of what Global Threat Intelligence does at machine speed. We need both in order to defeat cyber adversaries, whose aim is to harm our way of life.

Existing public/private partnerships should ensure that senior corporate and government officials are positioned to share vital information and best practices. Among other things, this means access to sensitive (or classified) information and a secure mechanism for sharing it.

Broad-based situational awareness is vital to securing our global cyber systems and ensuring our national security. Policies that enable companies and governments to work together, using global threat intelligence (e.g., combining cyber, energy, finance and other data) to enhance correlation and predictive capabilities, are critical to real-time responsiveness within the network switching/routing fabric. The Lieberman-Collins-Carper bill supports such information sharing by requiring the government to share information, including threat analysis and warning information, with owners and operators regarding risks to their networks. Legislation developed in the House of Representatives would benefit from similar language.

Conclusion

The cyber security challenge faced by our country is a serious matter that requires an evolution in the way in which both the public and private sectors collaborate. Each sector has its own set of core capabilities; only the government can implement the complex set of organizational and policy responses necessary to counter the growing cyber security threat. Leading information technology companies and their customers are uniquely positioned to act as early warning systems that can identify and help address cyber security attacks as a real-time cyber immune system.

With the right industry-government collaboration, networks of the future can comprise intelligence and create resiliency by instantly rejecting harmful code in milliseconds as opposed to the hours it traditionally takes to make a signature, just as our bodies reject viruses even though we may not know the name of the particular disease. Information technology companies focused on cyber security in particular have the resources and the

economic incentives to continue to invent and develop the technologies and solutions needed to stay ahead of sophisticated cyber attackers. In the best American tradition of collaboration, the public and private sectors have made important strides to address the cyber security challenge and to enhance trusted working relationships. As we work together to further evolve our collaboration models, we can succeed in protecting our homeland from the threat of cyber attacks.

Thank you for asking me to take part in this hearing on behalf of McAfee. I would be happy to answer your questions.