STATEMENT OF DR. PHYLLIS SCHNECK

VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER, GLOBAL PUBLIC SECTOR

MCAFEE, INC.

BEFORE:

UNITED STATES SENATE

JUDICIARY COMMITTEE

SUBCOMMITTEE ON CRIME AND TERRORISM

"CYBER SECURITY: RESPONDING TO THE THREAT OF CYBER CRIME AND TERRORISM"

APRIL 12, 2011

Chairman Whitehouse, Ranking Member Kyl and other distinguished members of the Subcommittee, thank you for requesting McAfee's views on responding to the threat of cyber crime and terrorism. Your subcommittee is playing a vital role in helping define the contours of the cyber security debate by investigating how we can defeat sophisticated syndicates of terrorists and criminals who deploy cyber attacks to finance their operations and undermine the security of our country.

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 (NCFTA), a partnership between government, law enforcement, and the private sector for information analytics that has been used to prosecute over 300 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. Prior to 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.

Before discussing McAfee's views on security, I want to note that McAfee also takes privacy very seriously – both in terms of our customers' information and that of the systems and networks we secure. We are committed to abiding by privacy laws and directives in the multinational jurisdictions in which we do business. We also believe that by researching and implementing cutting edge technologies to secure information and systems, we are providing the foundation for privacy protection, which is good, strong security.

My testimony will focus on the following key areas:

- McAfee's commitment to partnering with the law enforcement community;
- The evolution of the cyber security threat landscape;
- McAfee's Technical Response to the Cyber Crime Challenge – Whitelisting and Global Threat Intelligence;
- Two major cyber security attacks, Operation Aurora and Night Dragon, and their implications for our nation's security; and
- Policy recommendations to support law enforcement and 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.

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.

Evolution of the Cyber Security Threat Landscape

Traditionally, cyber crime has been associated with criminals using electronic means to obtain unauthorized access to financial information or money. Over time, the criminal landscape has evolved to include theft of intellectual property, network activism (e.g., distributed denial of service, or DDoS), and the destruction of critical infrastructure. Furthermore, the profit model continues to evolve and is getting even more lucrative for

cyber criminals, with a low barrier to entry and the prospect of significant monetary or strategic gains.

The evolving nature of cyber crime, and the context in which it operates, informs the way we define our company's strategy and design our products. My testimony, therefore, seeks to shed light on the way we think about cyber crime, how we drive the innovation of our products, and how we partner with the government to help make our country's networks and systems more resilient.

McAfee's Commitment to Partnering with the Law Enforcement Community

McAfee has a long history of collaborating with law enforcement at the global, federal, state and community levels, and our employees take great pride in this fact. Within the law, McAfee has assisted federal, state, and local police officials, supporting their investigations and prosecution of cyber criminals. We have worked to build strong working relationships with the FBI, U.S. Secret Service, state and local police, and governments worldwide that enable smooth, bi-directional communication both in times of crisis and during periods of normal operations. We help bridge these relationships for customers and partners by placing a particular focus on ensuring that coordination takes place when cyber events are occurring. In addition, we work to educate and get McAfee-developed information to law enforcement as quickly as possible.

As previously mentioned, I personally support law enforcement's efforts in cyber security, having served for eight years as chairman of the National Board of Directors of the FBI's InfraGard™ program, and chairing for the past 10 years the Board of Directors for the National Cyber Forensics and Training Alliance. NCFTA is a non-profit organization that co-locates critical infrastructure fraud analysts with law enforcement to engage data analysis and collaboration between public and private sectors while also preserving chain of custody of any findings so they may be used by law enforcement in court. The work within NCFTA has led to over 300 arrests of cybercriminals worldwide.

McAfee also has played an active role in the Department of Homeland Security's (DHS) Cyber Storm 1, 2, and 3 exercises to enable the Department to model cyber attacks and improve their ability to respond to them. We collaborate closely with DHS and the National Cyber Security Alliance (NCSA) to educate consumers on cyber crime, and have developed a free citizen scanner to help citizens gauge their risk of online crime victimization. We maintain a free website that we have offered to the U.S. government to host as part of their cyber security awareness activities related to a national campaign, "Stop.Think.Connect." In addition, McAfee supports 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 that facilitate a safer and more pleasant experience for electronic transactions.

In addition to these activities, 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. This 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 initiative include:

- Education and Awareness – McAfee works to ensure that officials around the world have the understanding and 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.

As part of our program, we maintain relationships with law enforcement communities around the world to facilitate information exchange, and we have trained numerous officers on malware creation and detection. What's more, we have provided grants to such key cybercrime fighters as the National White Collar Crime Center in the U.S. and the Council of Europe for its work on the Cybercrime Convention and outreach.

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 according to the will of the malware owner, such as providing unauthorized access to information or systems that control physical/kinetic infrastructure. To put it simply, 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. Upon detecting a virus, a security software vendor develops a signature and deploys it in the form of a file downloaded to the security software on customers' computers. That software is then 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 defense 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 – known as 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 – known as a "botnet."

Criminals and nation states can 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 – which is why we refer to this type of code as a worm. Thus 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, hackers are able to extend the time period in which their malware remains undetected and are 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 and that can insidiously send information back indefinitely before being detected.

Modern malware, therefore, 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. And 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's Technical Response to the Cyber Crime Challenge: White Listing and Global Threat Intelligence

Because the traditional "signature" model for antivirus, analogous to requiring a vaccine for every piece of malware, is no longer effective to combat swiftly moving cyber adversaries, more advanced defenses are needed. To win back our network resiliency requires not only strong public-private collaboration, but also that we move at machine speed – at the speed of light – and that we stay ahead of the adversary. Thus the two most critical innovations for the future of cyber security are application whitelisting and global threat intelligence.

Whitelisting

Instead of relying only on preventing malware from entering a machine or requiring prior knowledge of a piece of malware (via anti-malware software or signature-based "blacklisting" products), whitelisting changes the entire paradigm. Whitelisting (also known as application whitelisting) simply does not permit the execution of any instruction set that has not been previously approved. Thus, even though the adversary may in fact be able to get malicious code onto a machine, that machine, if equipped with whitelisting technology, will never execute the malicious instructions. The analogy in biology is exposing a person to a disease that will never be able to develop or harm the person.

Whitelisting technology enables organizations to be much more proactive in protecting their systems. Trusted applications, system components, and executables are identified and explicitly allowed. All other software or executables are denied by default. The technology is used to protect servers, endpoints, embedded devices and mobile devices. Significantly, whitelisting can also protect the integrity of many ATM's, point-of-sale terminals, and Supervisory Control and Data Acquisition (SCADA) systems, which, because

of resource constraints, often might not support traditional anti-malware software.

Global Threat Intelligence (GTI)

The second critical technology in proactively fighting cyber crime is known as 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 called Global Threat Intelligence, or GTI. GTI is the basis of a cyber immune system: the ability to protect against an attack by electronically detecting – via correlation at machine speed – cyber behavioral data from worldwide sources that is identified as harmful, long before a signature or name might be developed at human speed. The biological analogy is the human body defending against a potential disease simply because the body detects that the behavior is harmful.

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 either the IP address from which it originates, the web site, or other elements associated with the content in question. Thus cyber security providers can offer solutions enabling the customer to stop content that has 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's Global Threat Intelligence service, as well as a number of our other products and services, helped us first detect and then remediate two important recent 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 global companies (many of which were American) in the information technology, defense, and energy sectors – strategic industries vital to the country's long-term economic success and national security.

Two major cyber security attacks: Operation Aurora and Night Dragon

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 automatically be compromised and malicious code 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, the attackers would identify and compromise repositories of intellectual property and exfiltrate 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 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 Operation Aurora, 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 (a code injection technique that exploits a security vulnerability in the database layer of an application); 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. 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

As the previous examples demonstrate, combating cyber crime requires constant vigilance and sophistication on the technical side. The same is true for the law enforcement side – on which the burden falls for prosecuting such crimes. Yet law enforcement continues to lack the tools and resources needed to effectively train for and respond to cyber crime. And law enforcement's ability to seek and receive funding is often hampered by the difficulty of quantifying cyber crime. We therefore urge Congress, even in this period of budget austerity, to support the funding requests of our nation's law enforcement organizations, which are dedicated to fighting cyber crime.

In addition to more resources for law enforcement, we need more information sharing. 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 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 and are willing to share in the name of the greater good transcending competitive boundaries. Private companies need protected ways to share their big picture research findings more rapidly 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.

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, (S.413), 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.

The U.S. Government has made tremendous progress in the past two years in building international relationships to enable better prosecution of cyber criminals. A policy framework that further supports the expansion of these relationships throughout our community of allies would help reduce the profit model for cyber criminals by making punishment more likely. Technical innovations such as whitelisting and global threat intelligence increase the barriers to entry and decrease the chance of success of a cyber-threat reaching or hitting the target. The correct blend of technology and policy will greatly diminish the reward model for cyber crime worldwide.

Conclusion

The cyber security challenge faced by our country is a serious matter that requires an evolution in both technology and the way both the public and private sectors collaborate. In order to mitigate the cyber adversary, intelligence must be collected and shared among machines – at the speed of light – and also among people. Each sector has its own set of core capabilities. Thus 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 participate in this hearing on behalf of McAfee. I would be happy to answer your questions.