

STATEMENT OF
DR. PHYLLIS SCHNECK, VICE PRESIDENT AND CHIEF TECHNOLOGY OFFICER,
PUBLIC SECTOR,

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

SUBCOMMITTEE ON COMMUNICATIONS AND TECHNOLOGY

**“CYBERSECURITY: THREATS TO COMMUNICATIONS NETWORKS AND
PRIVATE-SECTOR RESPONSES”**

FEBRUARY 8, 2012

Good morning Chairman Walden, Ranking Member Eshoo, and other members of the Subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer-Global Public Sector for McAfee. We appreciate the Subcommittee's interest in cyber security as it affects the communications sector, as well as your interest in the private sector's response.

My testimony will focus on the following key areas:

- Today's cyber security threat landscape
- The communications sector's unique role in cyber security
- Private sector technologies such as Application Whitelisting and Global Threat Intelligence that are reducing the profit model of the cyber adversary
- Policy recommendations to encourage public-private sector information sharing at both human and machine speeds -- essential for responding to the modern cyber security challenge

First I would like to provide some background on my experience and on McAfee.

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 my role with 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 400 cyber criminals

worldwide. Previously, I served as Vice President of Threat Intelligence at McAfee and was responsible for the design and application of McAfee's™ Internet reputation intelligence, a system of real-time risk indicators. I have also served as a Commissioner and working group co-chair on the public-private partnership for the Center for Strategic and International Studies (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, building our relationships between FBI, DHS and other organizations and growing the InfraGard program from 2,000 to over 33,000 members nationwide. Prior to McAfee, I served in several executive roles in the security industry and also started and sold a business of my own in the security space. I also worked for several years at the MITRE Corporation in telecommunications network pricing algorithms. 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.

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 150 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Today's Cyber Security Threat Landscape

We face a transnational cyber adversary that is smart, fast, and has no legal, intellectual property, international or competitive boundaries. This adversary is often well funded, with no impediments to swift execution, and one of the most

effective ways to defeat this adversary is through the light speed communications infrastructures owned and operated by the Internet Service Providers (ISPs).

The cyber security threat landscape has changed fundamentally over the last decade as cyber threats have become increasingly more sophisticated and targeted. What had been science fiction is now reality: malicious actors perpetrating cyber attacks that steal money and intellectual property, disrupt businesses, sabotage critical infrastructure, and/or threaten governments and nation states. In fact, the past few years have demonstrated the largest known movement of money, markets, and jobs between countries and companies, all facilitated by cyber intrusions. Because global cyber connectivity enables all of this activity, it creates difficulties for attribution and punishment. This must change. A recent report McAfee released in conjunction with the Security & Defence Agenda (SDA), the leading defense and security think-tank in Brussels, found that 57% of global cyber security experts believe an arms race is taking place in cyber space, and 45% believe cyber security is as important as border security. Many governments around the world – including the U.S. – have acknowledged that cyber threats can be every bit as menacing as physical threats to a nation’s security, and the U.S. military, for example, has declared cyberspace a realm that warrants protecting.

McAfee Labs’ most recent threat predictions include an increase in attacks on smartphones and mobile devices. Attackers have moved on from simple destructive malware to spyware and malware that makes them money, exploiting vulnerabilities to bypass system protections and gain greater control over mobile devices. Researchers also predict that 2012 will see a move toward mobile-banking attacks.

Not only the kinds of attacks but the kinds of attackers have evolved as well. Cybercrime perpetrators have morphed from simple, low-budget hackers into well-financed criminal operations that contribute to a multi-million dollar cybercrime industry. Not all cybercrime has a financial incentive, however. Cyber criminals now include those interested in stealing intellectual property, personal/professional information and state secrets, gaining access to a nation’s entire slate of cyber processes, compromising critical infrastructures, advocating a cause (“hacktivism”), and/or launching a terrorist attack.

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 to hackers indefinitely before being detected.

Modern malware, therefore, can no longer be classified by its perceived purpose or propagation method, because both can change in an instant. Some types of software can be engineered to gain access to and maintain control over a 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.

Today, malware developers combine web, host, and network vulnerabilities with spam, rootkits (invisible malware that hides within authorized software in a computer's operating system), spyware, worms (which target computers rather than software programs but which can clog communications bandwidth and overload computers or networks,) and other means of attack. Malware also can be distributed indirectly by networks of computers that have been corrupted by a criminal – known as a "botnet," or a collection of compromised computers connected to the Internet.

Then there is the type of attack known as an Advanced Persistent Threat (APT), which is essentially an insidious, persistent intruder meant to fly below the radar screen and quietly explore and steal the contents of the target network. In the past two years, McAfee has uncovered numerous APTs affecting tens of thousands of organizations worldwide. Three of these large scale but quiet espionage operations drew particular attention – Operation Shady RAT, Operation Aurora, and Night Dragon. These attacks are significant because they were managed by coordinated, organized teams that succeeded in extracting billions of dollars of intellectual property from leading global companies in the information technology, defense, and energy sectors – strategic industries vital to any country's long-term economic success and national security. These low-profile attacks are often more dangerous than the high-profile incursions because they are a type of cyber espionage, providing silent, ongoing access to protected institutional information. And these APTs are not limited in scope; they can affect any company, government body or nation, regardless of sector, size, or geography.

The Communications Sector's Unique Role in Cyber Security

ISPs are foundational to all electronic communications activity. As such, they depend on hardware and software vendors to supply highly secure products and services to ensure that their systems are protected from a wide variety of attacks, particularly APTs. ISPs have, and will continue to demand that their vendors supply them with ever more secure products and services.

We also believe that ISPs can work even better with more situational awareness and a greater ability to correlate events within and beyond their own data. They can influence the market through the acquisition of systems and technology innovations

that address resiliency through blocking the execution of malicious instructions, as we describe later in this testimony. Finally, ISPs cannot carry the burden alone, and all systems should follow these premises. Cyber resiliency assumes the adversary will get in and that this will not be detrimental. This assumption can only be realized in a system that can detect and deter malicious instructions.

Internet Service Providers form the literal backbone of global communications. All Internet traffic is enabled at some point by an ISP – even the traffic of the malicious actors. Since ISPs haul the packets, it is the hope that others in industry can partner with ISPs to enhance technology and policy so as to eventually prevent the enablement of cyber adversaries, as well as to harden the ISPs and CIKR (Critical Infrastructure and Key Structures Resource Center) even further.

It's not just businesses, organizations and individuals who are at risk, of course. The cyber risk to our nation's critical infrastructures is real, and fortunately, policy makers are becoming more aware of the need to protect such vital systems as energy, water, transportation, and finance from cyber incursions. The communications sector is unique among critical infrastructures, however, in that it is the delivery mechanism for voice and data – including data from malicious actors. The Internet was architected to ensure that information arrives at the destination specified by its sender. Therefore, the Internet currently ensures the delivery of malware, leaving the receiver responsible to identify and prevent entry and/or damage from the malicious instructions upon arrival. Criminal actors, whether abusing the networks with botnets and other unsavory activity, or simply communicating, rely on communications networks just as much as law enforcement agencies checking a suspect's record in a federal database. Thus high-speed communications networks and ISPs become the agnostic enablers of both sides of the Information Age's equation.

Telecommunications companies are no strangers to network security practices. For years they have been working to keep their networks robust and secure. But the universe of online players is now so vast and interconnected, and the cyber threat is growing so rapidly, that even more is required. ISPs are under continuing pressure to provide “clean pipes,” a term used often in the industry for the delivery of traffic that has been “cleaned” of potential threats. From a strictly technical perspective, many ISPs have the ability to detect threats and remove some from the traffic before it is passed on. They could technically also check that routes have not been modified. However, when one considers other factors– such as cost, customer attitudes toward privacy, and ISP liability – the right answer is neither clear nor simple, especially at speeds of hundreds of gigabytes per second between ISPs and users.

The prize goal is to remove dangerous traffic instead of ensuring its arrival at its sender-specified destination. However, this requires several additional steps, such as global situational awareness, enabling the legal and policy framework, and a business case with clear return on investment.

ISPs and other telecommunications providers currently confront a wide array of federal, state, and international regulations that complicate their task of cleaning the pipes. The *Stored Communications Act of 1986*, for instance, often prevents ISPs from disclosing information about communications outside of their organization. This is just one example of a complex web of rules that have the effect of creating an environment of disincentives for ISPs and other telecommunications providers to collaborate with security companies in addressing the cyber security challenge.

ISPs are also confronted with financial disincentives that limit their ability to address this challenge. According to a major study done by the Institute for Homeland Security Studies, “An Economic Analysis of ISP Provided Cyber Security Solutions,” most customers are willing to pay only \$5 extra per month to receive an appropriate level of security. Thus ISP firms are forced to work within very tight margin constraints. Their customers are willing to pay a small amount to protect their own data but are not willing to pay extra to address the larger, structural security challenge: the reality that cyber attackers abuse the network to inflict attacks on a wide variety of targets.

This is a classic commons problem, and thus it is appropriate for government to work to address it, given governmental interest in reducing the threat of cyber attacks on the entire system. The types of positive incentives put forth by the ISP community – the types of positive incentives that we, too, support – do in fact make sense and are entirely appropriate for policymakers to consider. The entire Internet eco-system – from the core of the network to the enterprise edge to the individual systems and hardware, from ISPs to users, from the government to private sector experts – needs to be involved to combat the growing cyber threats that we as a nation face.

Private Sector Innovation: Two Proactive Technologies

The good news is that innovation in the private sector is vibrant, and is enabling security providers to address APTs, botnets and other incursions. 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. 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.

Two of these technologies are application whitelisting and Global Threat Intelligence. Both represent a new paradigm in cyber defense in that they are proactive and predictive, respectively, rather than reactive.

Application Whitelisting – Preventing the Execution of Malicious Instructions

The concept of application whitelisting flips the traditional antivirus model from one that identifies and attempts to block all malicious code (a concept known as blacklisting) to one that understands that the adversaries will get in but can be prevented from executing. This technology allows only good, pre-approved code to enter a system. Whitelisting instructions reside at the operating system level and simply do not permit the execution of any instruction set that has not been previously approved. Technologies based on whitelisting allow organizations to identify in advance only the software and executables that are permissible for downloading and executing on their systems. All other applications, such as malicious software, are denied by default.

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. The germ remains dormant, as do the malicious instructions in a machine protected by application whitelisting. Whitelisting technology enables organizations to be much more proactive in protecting their systems. The technology is used to protect servers, endpoints, embedded devices and mobile devices. Significantly, whitelisting can also protect the integrity of many ATMs, point-of-sale terminals, and Supervisory Control and Data Acquisition (SCADA) systems, which, because of CPU and performance resource constraints, often might not support traditional anti-malware software.

Global Threat Intelligence – Helping ISPs to Not Route the Traffic of the Adversaries

McAfee and other sophisticated cyber security providers have developed a technology that is unique in that it is predictive and not reactive. It enables multi-vector, real-time, predictive protection against the 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 and correlating, at machine speed, cyber behavioral data from worldwide sources that is identified as harmful – long before a traditional anti-virus "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.

McAfee's GTI uses 160 million sensors to span the Internet, continually seeking and identifying new and emerging threats before they materialize. To interpret this data, McAfee dedicates more than 350 researchers in 30 countries to focus exclusively on tracking and analyzing threat information, providing the most relevant security information 24x7. For instance, through global sensors researchers can note the prevalence of a new behavior and its propagation pattern and pace as it progresses through different countries, different types of users, or different delivery mechanisms. In milliseconds, GTI can assess changes, assign risk levels, and

distribute protection recommendations to products covering every threat at every tier.

Cyber security solutions based on this GTI approach protect computers by calculating the potential risk of a piece of content based on experience with either the IP address from which it originates, the website, or other elements associated with the content in question. Thus solutions can be offered that enable customers to be warned that, in the GTI provider's view, the content is too risky to be loaded into the memory of their computer.

ISP's currently address certain botnets with traffic flow data, but only those botnets that the ISP can see with the cyber intelligence they have. Collecting data from multiple sources would enhance the situational awareness picture and allow those who transport our traffic to see botnets that may be too dispersed to be noticed immediately with conventional traffic flow data. When used effectively, GTI technology can prevent the routing of traffic from bots and/or assist with the identification of infected machines that may be customers of the ISP, allowing the ISP to explore ways to help those customers clean the malware off their systems.

Technologies such as GTI – and others that are just now being developed – can actually decrease the profit model for cyber criminals across the spectrum, from the hacker hobbyist to the espionage or APT players. There is often overlap in the infected resources used, and application of collaborative GTI from multiple sources at the ISP can reduce the malicious traffic that is routed, leaving an Internet that is no longer a reliable transport system for danger. This is one reason McAfee believes that any national cyber security plan must involve the private sector – not just at the beginning, but at every stage.

Policy Recommendations

In general, we believe that positive incentives are superior to regulation in achieving the desired national outcome: a cyber secure nation. Using positive incentives rather than negative ones, such as government mandates, is the most effective way to drive higher levels of trust and actual cooperation between the private sector and government – all vital to producing real success.

Fortunately, we are not starting from scratch. There are a variety of approaches focused on positive incentives in play. Many of the recommendations of Representative Thornberry's (R-Texas) Cyber Security Task Force are a step in the right direction in that they address a wide range of incentives such as information sharing, insurance reforms, and tax credits. And over the past few years there has been good bipartisan collaboration on a number of cyber initiatives, including additional investment in cyber security research and FISMA reform, to name just a few.

In this same spirit, the information sharing bill introduced by Representative Mike Rogers (R-Michigan) and co-sponsored by Representative Dutch Ruppersberger (D-Maryland), the *Cyber Intelligence Sharing and Protection Act of 2011* (H.R. 3523), would be particularly effective in encouraging the kind of public-private partnerships we need to move forward in cyber security. An amended version of this bill passed the House Intelligence Committee in December with overwhelming bipartisan support. The premise of the bill matches our own on this issue: that government can facilitate collaboration and encourage trusted working relationships to the benefit of all parties in the Internet ecosystem.

H.R.3523 gives the federal government new authority to share classified cyber threat information with approved companies so they can better protect themselves and their customers from cyber attacks. The bill also empowers participating businesses to share cyber threat information with others in the private sector and enables the private sector to share information with the government on a voluntary basis. Importantly, the legislation also provides liability protection for companies that choose to protect their own networks or share threat information. Equally important, the bill includes vital protections for privacy and civil liberties - we are working to strengthen these provisions without weakening the important cyber security advancements it promises - and does not create any new federal spending, regulations or unfunded mandates.

Better enabling information sharing as outlined in Representatives Rogers' and Ruppersberger's bill is critical for addressing the cyber threat. This would help organizations execute with the alacrity shown by our cyber adversaries, as previously described. There are also other positive incentives that can help address some of the fundamental challenges ISP's, telecoms and other members of the communications eco-system have - challenges in hiring the right type of cyber security experts, regulatory disincentives, economic disincentives, and the immaturity of the insurance market, which has limited the growth of the kind of insurance programs needed for companies to insure against catastrophic losses:

- **Litigation/Legal Reform:** Imposing limitations on liability for damages as well as for non-economic losses would remove a serious obstacle to information security investments—i.e., the risk of losses for which responsibility is assigned notwithstanding a company's good faith investments in adequate information security. Eliminating that risk, at least for companies that meet high, "best practices" security standards, would encourage more security on a company-by-company basis. This approach can help create positive incentives for disclosure through liability relief for responsible organizations to improve the nation's overall cyber security posture.

- **Competitions, Scholarships, and Research and Development Funding:** Cyber security competitions and challenges, as well as scholarship and creativity to programs, can help identify and recruit talented individuals to the field to augment the future cyber security workforce. Similarly, research and development grants

foster innovation and advance basic and applied solutions. Recognizing this, several legislative proposals under consideration contain provisions designed to help industry meet the cyber security challenges of tomorrow and train the next generation of experts.

· **Tax Incentives:** Accelerated depreciation or refundable tax credits are being considered to encourage critical infrastructure industries to make additional investments in cyber security technologies, solutions, and human capital. The same approaches could be effectively applied to small businesses. Despite the current environment where balancing the budget is a critical priority, we cannot afford to be shortsighted. Cyber security-related tax incentives would prove to be a legitimate, long-term investment in security that would protect our national security and economic interests.

· **Insurance Reforms:** Many companies defer investments in improved security out of a concern that, even with improved security, they are not protected from liability for losses that occur. Similarly, insurance carriers are reluctant to create a vigorous marketplace for cyber-security insurance, thereby hindering investment. Government should give consideration to implementing reinsurance programs to help underwrite the development of cyber security insurance programs. Over time, these reinsurance programs could be phased out as insurance markets gained experience with cyber security coverage.

Conclusion

ISPs play a foundational role in the global digital infrastructure. Industry and government should work together to help ensure that ISPs gain access to and use the most innovative technologies available to protect our networks and citizens from increasingly sophisticated and insidious cyber threats.

Collaboration and cooperation between the public and private sector are key to addressing cyber security in a holistic way. By combining government and industry's threat intelligence, communications networks of the future can create resiliency by rejecting harmful code in milliseconds just as our bodies reject viruses reflexively, without knowing the name of the particular disease they are fighting. Government can promote innovation of these tools with the use of positive incentives. The resulting advances will be critical to protecting our networks, communications, intellectual property, state secrets, critical infrastructure and national security. In the best American tradition of collaboration, the public and private sectors have made important strides already to address the cyber security challenge and enhance working relationships.

We acknowledge the tremendous legal and challenges currently faced by ISPs in sharing threat intelligence and encourage policy makers to enable ISPs to provide more of their threat picture to other public and private entities in exchange for the respective data from others. This can then be used to block the most harmful threats

from being routed to their intended destination. Unlike the biological or weather models, we can block the harm once we detect it.

ISPs are not solely responsible for cyber resiliency, and we encourage all system owners and operators to protect their network assets with technologies like those mentioned, which can detect and prevent harm even in computer hardware and memory. Many industries have a large role to play in protection, innovation, and the advancement of good science.

We believe our public and private collective goal for ISPs is to enable the ISPs to protect, learn, and innovate with us, based on a legal, policy, and business framework that promotes cyber resiliency, civil liberties, and good business around the world. We look forward to participating in the ongoing efforts to maintain the resilience of our communications networks, which are so vital to every facet of the nation's economy and overall prosperity.

Thank you for requesting McAfee's views on these important issues. I will be pleased to answer any questions.