STATEMENT OF THE SOFTWARE & INFORMATION INDUSTRY ASSOCIATION

DR. PHYLLIS SCHNECK, VICE PRESIDENT FOR McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON SMALL BUSINESS

SUBCOMMITTEE ON HEALTH CARE AND TECHNOLOGY

CYBER SECURITY: PROTECTING YOUR SMALL BUSINESS

DECEMBER 1, 2011

Good afternoon Chairwoman Ellmers, Ranking Member Richmond, and other members of the Subcommittee. I am Phyllis Schneck, Vice President and Chief Technology Officer-Global Public Sector for McAfee, testifying on behalf of the Software & Information Industry Association (SIIA). We appreciate the Subcommittee's interest in cyber security as it affects small business, which plays such a large part in the nation's economy.

My testimony will focus on the following key areas:

- The national security implications of protecting small business from cyber attacks
- Today's cyber security threat landscape
- Practical steps small businesses can take to protect themselves from cyber attacks
- Policy recommendations to support the small business community 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 some background on my experience, on McAfee and on SIIA.

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 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.

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.

SIIA's Role in the Technology Sector

SIIA is the principal trade association of the software and digital information industry, with more than 500 members that develop and market software and electronic content for business, education, consumers and the Internet. As leaders in the global market for software and information products and services, many SIIA members provide products and services that protect businesses, consumers and the

public sector from cyber-attacks, viruses, and a wide range of online security threats. While SIIA's members include many of the largest and well-known businesses in the technology industry, our membership is largely comprised of small and medium-sized companies that are the focus of this Committee.

The Critical Role Small Business Plays in the Nation's Cyber Security

In a recent op-ed in *The Washington Post*, Harvard Professor Jack Goldsmith refers to the Pentagon's claim that it will defend the country against large-scale cyber attacks. He observes, however, that small-scale cyber exploitations are far more common and actually pose a more serious national problem, as they are designed to copy or steal information, exploiting valuable government and business secrets. So-called small-scale incursions and are vastly more pervasive than cyber attacks, Professor Goldsmith states, and thus constitute a more serious threat to the nation's security.

Having investigated a number of cyber infractions over the past year that systematically drain companies' sensitive information, I wholeheartedly agree that often the more dangerous threat is not the high-profile, large-scale "hack" but rather the low-level incursion that sinks below the radar screen. Some of these constitute what security professionals call an Advanced Persistent Threat (APT), which I will discuss in more detail later, and the APT can affect organizations of any size. Small businesses are particularly vulnerable, as often cyber security is considered a "nice to do" rather than a "must do," sometimes because of budget constraints. Yet the intellectual property of a small business – let's say a small government contractor or an entrepreneurial start-up – can be just as critical to national security or the next technological innovation as that of a large enterprise.

The importance of small business to the national economy cannot be overstated. According to the Small Business Administration (SBA), small firms

- Represent 99.7 percent of all employer firms
- Employ about half of all private sector employees
- Pay 43 percent of the nation's private payroll
- Have generated 65 percent of new jobs over the past 17 years

Significantly, small firms also hire 43 percent of all high tech workers and produce 16.5 times more patents per employee than large patenting firms. Thus they are equally important to the country's collective intellectual property. Small businesses have a wealth of information – from both the public and private sectors – that could be quite valuable to a foreign nation or enterprise. And of course many of the country's most successful large businesses, such as Apple and Google, started out as small businesses.

It is also important to remember that small businesses are part of the U.S. infrastructure and network fabric, meaning that efforts to enhance the cyber security of small businesses contribute to the security posture of the entire nation. While small businesses have fewer resources to dedicate to cyber security, they face the same risk. And the risk is not just an IT risk but also a risk to the entire business. Thus we believe that managing a business's security ought to be the province of senior business leaders – not simply the IT department. As high-profile cases have demonstrated, cyber risks are growing in complexity and number.

Today's Cyber Security Threat Landscape

Today's cyber threats are more sophisticated and targeted than ever and are growing at an unprecedented rate, necessitating advanced protection and instantaneous remediation. McAfee Labs finds, for example, that both malicious URLs and malware have grown almost six-fold in the last two years, and that 2010 saw more new malware than all previous years combined.

Likewise, cybercrime perpetrators have evolved 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 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.

In the past year alone, McAfee has uncovered numerous cyber exploitations, three of which drew particular attention: Operation Shady RAT, Operation Aurora and Night Dragon. Each of these qualifies as an Advanced Persistent Threat (APT).

The most recent APT operation we uncovered, in July 2011, is known as Operation Shady RAT (for "Remote Administration Tool"). Operation Shady RAT has been stealing valuable intellectual property (including government secrets, e-mail archives, legal contracts, negotiation plans for business activities, and design schematics) from more than 70 public and private sector organizations in 14 countries. The list of victims ranges from national governments to global corporations to tiny nonprofits, and includes government agencies in the United States, UK, Taiwan, South Korea and Canada. The vast majority of victims (49) were U.S.-based companies, government agencies, and nonprofits. The category most heavily targeted was defense contractors (13).

As mentioned earlier, the APT is much more dangerous than the high-profile attack because it is an insidious, persistent intruder meant to fly below the radar screen and quietly explore and steal the contents of the target network. This kind of low profile but highly targeted threat is analogous to cyber espionage as it provides ongoing access to protected institutional information. Such quiet yet dangerous intrusions are not limited in their scope. They can affect any company, government body or nation, regardless of sector, size, or geography.

The onslaught of increasingly sophisticated targeted attacks is reflected in growing information breach statistics. A 2010 survey found that 60 percent of organizations report a "chronic and recurring loss" of sensitive information. More than one million small businesses and retailers were victims of some type of information theft in 2010. Physical theft or tampering with point-of-sale terminals was experienced by 37 percent, while computer viruses and malware were seen by 22 percent. Fifty-six percent of small and mid-sized businesses experienced some type of banking-related fraud in 2010, with 75 percent of this coming from online sources, most prominently online account takeovers. Among small businesses falling prey to bank fraud, 61 percent were victimized more than once.

While small businesses fall prey to the same security risks as large businesses, they generally cannot allocate large amounts of costly and scarce resources to security and compliance. Small firms cannot afford a dedicated security staff, nor do they have million-dollar budgets to purchase enterprise security solutions. Regardless, small companies must meet the same security and compliance requirements as Fortune 500 firms to remain in business. What's more, any business that experiences a security breach must spend increasing amounts of capital on investigations, individual notifications to persons with personal information exposed, strengthened security countermeasures and programs, and, increasingly, legal fees and fines. Then there are the intangible costs to reputation, brands, and goodwill — costs that, in some cases, can exceed the tangible costs.

Small Business: Maintaining Strong Security with Reduced Budgets

The average security budget for all companies is around 5 percent of the total IT budget, with some sectors, such as financial services, spending a considerably higher percentage. In the current economic climate businesses are generally spending less on their IT budgets. Yet security requirements continue to grow. The news is not all doom and gloom, however, because small businesses are often more creative in their approach to challenges.

A classic example of how small businesses can maximize their investments and get more bang for their security and compliance buck is demonstrated in the early adoption of three new security and industry trends—Software-as-a-Service (SaaS), managed security services, and dedicated security appliances. Both cloud-based services and security appliances offer new bundles of security and compliance functionality at lower prices than previously available. While these technologies were not well understood and initially were viewed as more risky when introduced, they both require far less time and capital to be deployed than traditional enterprise software solutions.

Small businesses have a deep and fundamental appreciation of the linkage between managing business risk and competitiveness. They intuitively understood the agility and economic benefits of cloud-based software and security services. Small businesses became early and enthusiastic users, launching the growth in SaaS and managed security services while propelling growth to double digits. The economics caught the attention of large enterprises that fueled a second wave of growth.

The trend to increased use of SaaS, cloud-based managed security services and dedicated security appliances is expected to further accelerate and outpace licensed software until it becomes "the preferred purchasing method."

Risk Management for Cost-Effective Security

Meeting tougher security requirements is not optional for any business, regardless of size. However, it is possible to have strong, effective security efficiently delivered at an acceptable cost – a fundamental requirement for small business. We recommend three guiding principles to make the cost of security most effective:

- Minimize the amount of sensitive information retained in the organization
- Practice risk management first
- Buy the appropriate level of security

I will say a little bit about the first two principles.

Minimizing the Amount of Sensitive Information

Many organizations have repositories of sensitive employee and customer data for internal use or to provide revenue-generating services, such as billing or insurance claims. Minimizing the types of sensitive information processed is not always an

option when the strategy of the business is to add value by processing finance, healthcare, or consumer information. However, where possible, efficiencies can be gained by reducing the number of locations where sensitive information is processed or stored. Consolidating systems and locations that process and store sensitive information reduces risk and the cost of protecting sensitive information in multiple locations.

A related strategy to sensitive data minimization is obfuscation. New technologies such as tokenization, or proven ones like encryption, require keys or indexes to make the information usable by humans. It can greatly reduce the cost of protecting sensitive information after consolidation. Risk is reduced because specific exemptions are allowed for breaches of encrypted information that eliminates the costly notification step.

Risk management for security and compliance

Experts across the security, compliance, and risk management spectrum agree that the most cost effective way to manage security and compliance starts with classic risk management. Compliance regulations require a periodic and documented assessment of risks to sensitive information. A risk management assessment is no longer optional for businesses covered by compliance regulations.

IT risk management brings an insurance paradigm to security and compliance. It is increasingly practiced in the public and private sectors, with a track record in producing cost savings, stronger security, and better compliance. Risk management is comprised of four phases:

- Identifying information assets
- Assessing threats and vulnerabilities
- Mitigating risk
- Monitoring and reporting

It is important to remember that security is a journey, not a destination. The security journey requires continuous monitoring of safeguards, critical systems and information, and new developments in the threat universe. It is also important for any business – particularly a small business – to choose a security partner that will help them make the most of their scarce resources.

Policy Recommendations

Very broadly, there are two schools of thought on government's role in achieving a desired outcome: one that posits that regulatory mandates are the best way to incent good behavior (in this case, strong cyber security measures); and, alternatively, one that asserts that positive outcomes are best achieved via positive incentives.

One might expect firms that make their living selling computer network security solutions to favor the former, a heavily regulatory model. Without question, a restrictive, sky-is-falling regime focused on mandates and elaborate regulation would compel organizations, across sectors, to spend lots of money on network security.

However, the heavily regulatory approach would not necessarily make organizations more secure – just more compliant. On the other hand, positive incentives have a higher probability of success in two ways: a higher chance of better actual outcomes, and a higher probability of producing legislative success. The private sector responds to incentives, and aligning the interests of the private sector with the outcomes that are in the national interest makes sense. Doing so could also provide rare proof that the phrase "win-win" is not always a cliché. Furthermore, positive incentives (rather than negative ones) are clearly the most effective way to drive higher levels of trust and actual cooperation between the private sector and government – vital things needed to produce real success.

Fortunately, we are not starting from scratch. There are a variety of approaches focused on incentives in play. The recommendations of the House Republican Cyber security Task Force are a step in the right direction, and there are a number of promising approaches in development on the Democratic side of the aisle as well. With the goal of encouraging collaboration and advancing an incentives-based approach to enhancing cyber security among small businesses, we support the following approaches:

- **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.

- **Public/Private Partnership on Information Sharing**: To further promote public/private partnerships, several existing models can be especially helpful. For instance, the Departments of Defense and Homeland Security manages many public/private partnerships, and McAfee plays a role in several. These partnerships are examples of success that should be emulated, as they aim to ensure that senior corporate and government officials share vital information and best practices.

- **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. Cybersecurity-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.

Government Attention to Small Business Cyber Security

While there is more that government could do to help small business fund effective security measures, I want to note some existing efforts that are headed in a positive direction.

McAfee is involved in the Federal Communication Commission's launch of the Small Biz Cyber Planner, an online resource to help small businesses create customized cyber security plans. This initiative represents a partnership among government agencies, industry groups, and private sector companies, and it is intended particularly for businesses that lack the resources to hire a dedicated cyber security staff. The tool will walk users through a series of questions to determine what cyber security strategies should be included in the planning guide, then create a customized cyber security template.

In addition, SIIA supports the recent effort by the Departments of Commerce and Homeland Security to create a voluntary industry code to address the detection and mitigation of botnets – malware distributed indirectly by networks of computers that have been corrupted by a criminal actor, turning the computers into elements of a robot network. We endorse the concept of a voluntary approach, in which the

government brings together relevant parties to confer on best practices to discuss how the private sector can develop and maintain timely and voluntary programs to detect and notify end-users that their machines have been infected with botnets or other malware and provide mitigation support that will eliminate these infections.

Another initiative that will benefit businesses of all size is the agreement between NIST, the Department of Education, and the newly formed National Cybersecurity Education Council to develop a strategic public-private partnership to promote formal cyber security education. This program is designed to help the National Initiative for Cybersecurity Education broaden the pool of skilled workers capable of supporting a cyber-secure nation.

Finally, collaboration and cooperation between the public and private sector are key to addressing cyber security in a holistic way. With the right industry-government collaboration, networks of the future can comprise intelligence and create resiliency by instantly rejecting harmful code in milliseconds just as our bodies reject viruses even though we may not know the name of the particular disease. Such advances – and others that I cannot even imagine right now – will be critical to protecting all sized businesses and organizations. In the best American tradition of collaboration, the public and private sectors have made important strides to address the cyber security challenge and enhance working relationships. We look forward to participating in the ongoing efforts to secure the valuable IP resources of our small businesses, large businesses and government, for as I hope I have shown through this testimony, all three are often connected.

Thank you for your interest and I will be pleased to answer any questions.