

**Statement of
Stuart McClure, McAfee, Inc.
Executive Vice President and Worldwide Chief Technology Officer**

**Before
United States House of Representatives
Committee on Homeland Security
Subcommittee On Oversight, Investigations, and Management**

“America is Under Cyber Attack: Why Urgent Action Is Needed”

April 24, 2012

Good afternoon Chairman McCaul, Ranking Member Keating, and other members of the Subcommittee. I am Stuart McClure, Executive Vice President and Worldwide Chief Technology Officer for McAfee. Thank you for requesting my views on this important topic.

You asked me to focus on the cyber threat, so my testimony will focus on threats to consumers, to intellectual property, and to critical infrastructure. During my discussion I will attempt to highlight the following points:

- The world’s continual drive to innovate has driven unprecedented connectivity which has given rise to exploding numbers of cyber threats and attacks.
- The only way to definitively solve this problem – and it is solvable – is through “security by design”
- There are policy initiatives, such as enhanced information sharing and other measures, that would dramatically help respond to these threats.

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

As Global CTO, I work closely with senior leaders at McAfee to ensure strong collaboration on customer requirements, knowledge sharing, strategy, development efforts, advanced threat research, and technology patents. Prior to joining McAfee, I held positions as executive director of security services for Kaiser Permanente, a \$34 billion healthcare organization; served as senior vice president of global threats and research at McAfee Labs, where I led an elite global security threats team; and was founder, president, and chief technology officer of Foundstone, which was acquired by McAfee in 2004.

I have dedicated my entire professional life to the practice of cyber security. My first book, *Hacking Exposed*, was published in 1999 and has been translated into

more than 30 languages and has become the definitive best-selling computer security book teaching the good guys how the bad guys think and attack. I have demonstrated literally 100s of hacker techniques in front of live audiences for the better part of 20 years, as I believe a picture is worth a 1000 words and a demo is worth millions.

McAfee's Role in Cyber Security

McAfee, Inc. protects businesses, consumers and the government/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 brings together more than 150 partners, large and small, to allow organizations access into our extensible management platform and thereby detect and prevent attacks in real time.

The Double Edge of Connectivity

Today, we are always on and always connected. The world of instantaneous communication and constant connectivity we have come to take for granted is limited only by our powers of creativity and innovation – and those seem to have no end. For years policymakers have heard of the numerous benefits that this interconnected, always-on world can and does bring to the areas of education, health and medicine, energy, and transportation, as well as to individual well being and the American economy at large. Indeed, the Federal Communications Commission has now redefined “universal service” from a program designed to create universal telephone service, to a program that will create nationwide high-speed broadband access. There is no turning back from this path, nor should we want to.

The reality, however, is that this same world of connectivity also creates risk. Risk is dictated by three factors: opportunity, motivation, and ability. If you are able to affect any one or more of these factors, you reduce the overall risk. In today's

environment, all three factors – opportunity, motivation, and ability – are growing inordinately.

Let me start with motivation. By now you have heard much about a variety of criminal actors who are highly motivated – either by money, national pride, religion, or some other compelling factor. These actors have huge amounts to gain with hardly anything to lose; our laws and penalties, in addition to our inability to enforce them, make cybercrime extremely attractive and profitable. There are few real deterrents to cybercrime and there is much to gain.

Add to this the fact that the level of ability of most cyber criminals has increased dramatically from the days of the pimply teenager working out of his garage. Now there are serious professionals and even companies for hire. Simply put, attacks are relatively easy to perform, leveraging thousands and even millions of computers to attack a single target, creating virtual armies that are far less expensive and more dynamic than physical armies. The tools and techniques are well documented, easy to find and the range of a malicious individual armed with a laptop and an Internet connection surpasses that of any ICBM.

Who has the opportunity? Certainly insiders – those with knowledge of the organization and its most sensitive data and systems – have optimum opportunity. But in the highly interconnected world, a cyber attacker certainly does not have to BE inside an organization to GET inside it. Indeed, almost any device that we use regularly – mobile phone, tablet, laptop, thumb drive, automobile, and even a medical device – is perfectly capable of letting an attacker inside. Anything that you can connect to, or that can be connected to – through USB, wired network connection, WiFi network connection, Bluetooth, RFID – is enough to let a cyber criminal in.

Yet the other great reality about a world that is becoming increasingly interconnected is the degree to which connected devices are helping individuals address significant challenges, and many of these challenges are highly personal. For example, diabetics can now use insulin pumps that are connected wirelessly; homeowners can set their burglar alarm or control the temperature of their homes remotely; patients with heart conditions can stay home while doctors monitor their conditions from their offices; students in rural areas can take classes at major universities; motorists can have their car's door locks unlocked from remote or be routed to their exact destination and soon might be able to drive on smart highways.

This list is by no means exhaustive. Innovative companies have every incentive to offer more and more goods and services addressing the most fundamental needs of consumers while at the same time make them more interconnected. This is a powerful market trend that will continue in the future. But unless the devices are locked down and secured by design, the cyber criminals will be given even more opportunities to profit, plunder, and pillage.

The Risk to Individuals and Consumers

Most consumers expect that when they go online, they will be safe, their information will be private, and their kids will be protected as long as they do not go on websites from which their parents have barred them. But this is an illusion. For every control, there is a bypass.

The threats that individuals and consumers face run the gamut from identity theft to loss of financial or personal information, to infection of their systems and destruction of hardware, software and data. The advent of new mobile technology, particularly smartphones and tablets, has opened up new attack vectors for hackers.

According to a recent House Science Committee witness from Idaho National Labs, Dr. Rangam Subramanian, every key economic sector will soon be dependent on wireless: energy and power, public safety, finance, health care, transportation, entertainment and more. Yet for all the convenience and innovation that wireless brings, it also introduces even more opportunities for hackers.

Many Americans now engage in personal banking, shopping, and other services by accessing Wi-Fi hot spots on their smartphones, which can lead them directly into traps set by cybercriminals. And the wireless revolution is only in its infancy. Cisco's US mobile data forecast projects that mobile data traffic will increase 16 times from 2011 to 2016 for a compound annual growth rate of 74 percent. By 2016, mobile data traffic will be equivalent to four times the volume of the entire U.S. Internet in 2005. The U.S. is a leader in the area of wireless innovation, and it is to our national advantage to have that leadership continue. The key is to ensure that that innovation incorporates security by design.

Following are just some of the most recent threats to consumers:

Social networking sites. The social networking phenomenon has overtaken pornography as the #1 Internet activity and has brought traditionally non-computer savvy users onto the Internet in droves. As an example, if Facebook were a country, it would be the 3rd largest in the world with over 850 million users. And cybercriminals know this. The attack surface area is large, but they might, for example, send what appears to be a harmless video but when clicked on it downloads a malicious virus.

Mobile devices. While PCs remain the bigger targets, smartphones -- which of course are miniature, mobile computers -- are quickly capturing cyber criminals' attention, with instances of mobile malware increasing by 600% from 2010 to 2011. McAfee Labs again saw the Android platform firmly ensconced as the number one target for writers of mobile malware. However, it is a misconception that Mac platforms are invulnerable to attack. As Apple recently learned with the Flashback Trojan, even their MacBooks can be victims, with over 600,000 infections to date. The hackers go

where the numbers are, and the more ubiquitous iPhones and iPads become, the more they will be targeted by hackers.

Mobile apps. In 2011, apps that appeared legitimate were bundled with malware and distributed over Google's Android Marketplace. Google was able to remotely detect and delete more than 50 infected applications from thousands of Android devices. Every day, consumers download apps from unknown apps stores without a second thought. We advise consumers to download apps only from well-known, reputable app stores, check reviews and apps ratings before downloading them, read the fine print to check what permissions the app is accessing, and install a comprehensive mobile security product, including those from McAfee or other vendors.

Phishing scams and IRS scams. During the tax season, in particular, hackers are known to conduct scams that involved phishing -- a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity. Some criminal actors masquerade as the IRS or an entity closely related to the IRS. We advise consumers never to respond to or click on links within unsolicited emails requesting that they enter personal data or visit a website to update account information – especially from the IRS, as they do not send out emails to consumers.

Perhaps one of the most unsettling examples of individuals being exposed to cyber attacks on a personal level entails the use of personal medical devices. Recently a McAfee researcher identified a security flaw in a wirelessly enabled insulin pump, which allows the device to be controlled by a hacker and subsequently administer a potentially lethal dose of insulin to diabetes patients. While there are several security holes in the device, the principal vulnerability comes from the wireless connection between the glucose monitoring system and the pump itself, which is vital to determining how much insulin is dispensed.

Since that story was publicized, I've heard from several friends who either used the pump in question themselves or whose child did. When they asked me if their pumps – and thus their lives – were vulnerable to cyber attack, I had to answer “yes.” Again, medical device manufacturers are making great strides in reducing inconvenience for individuals, yet at what price? Unless devices are built from the ground up with security by design, the price could be high.

Another example is automobiles. Many security researchers have noticed an alarming number of vectors of attack inside today's increasingly computerized cars. They have discovered that cars are as insecure as PCs were some 20 years ago, fraught with ways into the system and vulnerabilities to attack. In fact, researchers from the University of Washington and the University of California, San Diego, have released findings over the past two years detailing how they could not only open a locked car without the keys but they could remotely penetrate a car's IVI (in-vehicle infotainment) system to then take over control of much of the car's features,

including disabling airbag and brakes. Both these examples show that in our highly interconnected world, you don't have to be sitting at a computer or holding a smartphone to be vulnerable to cyber attack.

The risk to intellectual property

One of the most insidious types of threats to individuals, corporations, organizations, government agencies and the economy as a whole is the theft of intellectual property. 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 has received much attention recently. The APT 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 three years, McAfee has uncovered numerous APTs affecting tens of thousands of organizations worldwide. These attacks are significant because they were managed by well-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 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.

However, as the U.S. is the largest producer of intellectual property in the world, we are an especially rich target. 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. The average cost of a data breach reached \$7.2 million in 2010 and cost companies \$214 per compromised data record, according to the Ponemon Institute. And that's just the cost to respond internally to a data breach. If a company's intellectual property is stolen, it could decimate an organization.

We do not have statistics for all of the IP breached, as organizations can be reluctant to report IP theft, fearing that it will cause customers and markets to lose confidence. Again, by building products and systems that are secure from the

ground up, these fears, costs, and substantial drain of American competitive innovation could be greatly reduced.

The Risk to Critical Systems and Infrastructure

As policymakers have begun to recognize, a cyber attack – or series of cyber attacks – to the nation’s critical infrastructure could be tremendously devastating to our way of life. Let’s take the electrical grid, by far the most vulnerable of our critical infrastructures.

Almost every aspect of American life depends on electricity — from producing goods to saving lives, from defending the country to conducting electronic banking and commerce, from simple communications to feeding our families safely. Yet the systems used to manage our electricity, the supervisory control and data acquisition, or SCADA systems, are antiquated, running on commonly available operating systems, and with their design having changed little since their introduction decades ago. They were never designed or built securely, and they certainly were not meant to be connected to the Internet. And even today, we find that many electric companies still use vendor-supplied default passwords because they allow easy access in times of crisis or for maintenance and repair.

A report by CSIS and McAfee interviewing executives in the energy and power sector found that a large majority of them had reported cyber attacks, and about 55% of these attacks targeted SCADA. In 2009, nearly half of the respondents said that they had never faced large-scale denial of service attacks or network infiltrations. By 2010, those numbers had changed dramatically; 80 percent had faced a large-scale denial-of-service attack, and 85 percent had experienced network infiltrations. Meanwhile, a quarter of the interviewees reported daily or weekly denial-of-service attacks on a large scale. A similar number reported that they had been the victim of extortion through network attacks or the threat of network attacks. Nearly two-thirds reported they frequently (at least monthly) found malware designed for sabotage on their system.

Attacks on systems like SCADA can give hackers direct control of operational systems, creating the potential for large-scale power outages or man-made environmental disasters. Yet in the US, many companies have not adopted security measures for their SCADA systems, and many report their SCADA systems connected to IP networks or the Internet, making these systems even more susceptible to attacks.

What happens when there are multiple, simultaneous failures or system manipulations in the electric grid? Industry experts acknowledge that the grid is not currently equipped to handle this situation. While the experts say that the odds of a natural event or a physical attack creating this situation have been quite low, they are not prepared to say that for cyber – which all agree is the threat most likely to give rise to this kind of power failure.

What could happen? Imagine that cybercriminals have been gaining access to various parts of the power grid for years. They have infiltrated enough systems to make it possible to knock out power for the entire Northeast grid. They launch an attack in winter and power goes down throughout the area. Not only do people lose heat, light, refrigeration, cooking facilities, communication and entertainment, but the systems that pump our water from reservoirs – and those that purify the water in the reservoirs – are affected. No potable water, perhaps no water at all, and no capacities for managing sewage.

Even if stores have back-up generators, they cannot order the inventory because their systems are electronic. Banking comes to a halt because funds can no longer move electronically. Gas stations can no longer sell gasoline. Commerce effectively ends because order fulfillment systems are down, payment systems are down, and communication is down. Those consumers with phone service through the Internet – including those triple play plans offered by major providers – are out of luck because their service is no longer over the traditional landline telephone network. Hospitals and medical centers, which might also have independent generators, can care for only the most critical patients, as they cannot check on patients' insurance status or connect with the outside world electronically. While many of these sectors have emergency back-up systems to enable them to maintain operations during a power failure, those back-up systems are meant to be temporary – not long-term.

I personally experienced something like this as a child living on the island of Guam. A devastating and powerful typhoon knocked out power for many weeks and we had to run back and forth between the slowly moving water truck driving down the street and the house's bathtub where we emptied the bucket and ran back. The memory of that time is vivid, but it was not nearly as bad as it might have been had the situation gone on longer.

Security by Design

Adding security features into systems after they have been developed is a losing battle. Remember the sunroof of the 1980's? The only way to get one was to get it installed aftermarket. Manufacturers did not offer one as an option on new cars. And many of them leaked badly. Today, every manufacturer offers a sunroof as an option to your new car – and they never leak!

Cyber security has to be the same: it must be baked into the equipment, systems and networks at the very start of the design process. Security must be intrinsic to an organization's thought processes, its business processes, and its design, development, and manufacturing processes. It must be embedded in a product or network element so that it becomes an integral part of the product's or element's functioning. This approach is not only more effective; it is less cumbersome and less expensive than trying to lock down systems that are inherently insecure.

Policy Recommendations

Given the level of the cyber security threat, the government has a legitimate interest in ensuring that our country is protected from cyber attacks. The first order of business must be for the government to fully protect its own institutions, and we support rapid passage of FISMA reform legislation. The government also has an obligation to work with our companies and citizens to improve the level of security at work and in the home. I 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. Having the private sector fully commit -- customers and vendors of IT products and services -- to the principles and implementation of security by design will do much to help make our country more secure in the future.

There are a variety of legislative approaches focused on positive incentives in play right now that I believe can make a major contribution to addressing our country's cyber security challenges. 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, better information sharing would be particularly effective in encouraging the kind of public-private partnerships we need to move forward in cyber security. There have been several proposed government solutions, and many of them share McAfee's goal that government facilitate collaboration and encourage trusted working relationships to the benefit of all parties in the Internet ecosystem.

Better enabling information sharing 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 our nation's fundamental challenges— 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

As Global CTO for the world's largest dedicated security company, I carry a heavy burden, but one to which I have dedicated my entire career: to protect the world from cyber security attacks. But I stay focused on this task because I believe I can make a difference to provide a safer world for our children.

Thank you for giving me the opportunity to take part in this hearing on behalf of McAfee. 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. 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.

Aligning government incentives with a national objective of achieving security by design in all of our systems is consistent with the best American tradition of collaboration. The public and private sectors have made important strides to address the cyber security challenge. As we work together to further evolve our collaboration models, we can succeed in protecting our homeland from the threat of cyber attacks.