Summary of McAfee's Dr. Phyllis Schneck's Statement, May 21, 2013
Cyber Threats and Security Solutions – Energy and Commerce Committee

McAfee, an Intel company, works with many companies in the energy sector and does indeed have perspectives on the sector's threat environment. Energy is the infrastructure of infrastructures in that it supports so many others. At the same time, cyber is becoming the nexus and enabler of critical infrastructures, as more systems make use of the Internet, which puts the "smart" in smart grid, for example. This, of course, also opens up vulnerabilities.

Cyber bad actors are increasingly targeting energy, as incidents like Stuxnet and an apparent successor, Duqu, illustrate. Attacks on energy companies can be subtler than seeking to destroy physical facilities; they can be targeted toward gaining sensitive IP (a type of cyber espionage), or they can be extortion (80% of power companies in Mexico, 60% in India say this is most common cyberthreat).

Attempts to modernize energy distribution, say in the U.S., have brought together once separate domains – the equipment itself, the system control and data acquisition (SCADA) and the provider's IT network. If any one of those domains is connected to the Internet, they can receive malicious code from the Internet.
You don't have to attack with cyber directly, either, as the recent bank heists show. There humans hacked a database to get credentials (usernames/passwords), then used those to create fake bank cards and rob the ATMs. The cyber event was the initial database intrusion; the rest was done by humans.

Because of its vulnerability, the energy sector is regulated regarding cyber security. The problem is that sometimes that regulation is overly specific about a technology and ends up hindering rather than helping companies to be optimally secure. We urge the adoption of a faster review process, possibly an annual review of rules, and we also urge that regulations be outcome-based. For sectors not already regulated, we urge information sharing, innovation, and positive incentives.

Sharing real-time information about malicious codes between the government and private sector can make a real difference in our ability to thwart bad actors. But many in the private sector hesitate to share information because of concerns about liability. The Rogers/Ruppersberger bill, or something like it, would fix this and better enable public-private partnerships that NIST and DHS have already started. We hope sufficient privacy protections will help cement the broad coalition needed to make this bill law.

Innovation, such as treating networks as smart, adaptive ecosystems that both produce and consume intelligence about threats, is also key. McAfee calls this concept Security Connected – an open, dynamic, adaptable yet connected security platform. Positive incentives include tax incentives, liability protections for companies sharing information, insurance reforms, and R&D initiatives.

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

McAFEE, INC.

BEFORE:

UNITED STATES HOUSE OF REPRESENTATIVES

COMMITTEE ON ENERGY AND COMMERCE

"CYBER THREATS AND SECURITY SOLUTIONS"

MAY 21, 2013

Good morning Chairman Upton, Ranking Member Waxman, and other members of the Committee. I am Phyllis Schneck, Vice President and Chief Technology Officer, Global Public Sector for McAfee, Inc., a subsidiary of Intel Corporation. We appreciate the Committee's interest in cyber security threats and solutions, particularly as they affect critical infrastructures.

My testimony will focus on the following areas:

- The threat landscape for the energy sector
- The particular vulnerabilities of the energy sector
- The liabilities of regulation for cyber security in the energy and other critical infrastructures
- Security solutions: information sharing, innovation, and positive incentives

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.

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 am the Vice Chair of the Information Security and Privacy Advisory Board (ISPAB) and 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 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 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 160 technology partners—large and small businesses all committed to continuous innovation in security—have joined the alliance, with more to be announced soon.

Threat Landscape for the Energy Sector

It's hard to overstate the importance of securing the nation's power grid – a grid on which so many other of our critical infrastructures depend. The energy sector feeds water, agriculture, transportation, finance, communications, information technology, the military and homeland security, not to mention healthcare and education. It's no exaggeration to call energy the infrastructure of infrastructures.

At the same time, cyber is becoming the nexus and enabler of critical infrastructures -- especially energy – as more and more systems make use of the Internet. Cyber puts the "smart" in smart grid, for example. The problem is that the very thing that makes the grid smart—the ability of myriad embedded systems to communicate with each other, often using a combination of legacy and proprietary equipment alongside more modern

solutions—has expanded the attack surface, making it vulnerable to cyberthreats. Open systems invite hacking.

Attacks on the Energy Infrastructure are Growing

The story of Stuxnet is like that of a sensational crime that generates a flurry of media attention and speculation when it happens, but eventually fades from the news even though the mystery remains unsolved. The Stuxnet worm first came to the public's attention in 2010, when it attacked several facilities around the world, including Iran's nuclear enrichment infrastructure, taking control of programmable logic controllers that control the automation of mechanical processes and disrupting centrifuges and turbines.

Since then, more advanced variants of the malware have been reported in various places globally. In a 2010 survey on critical infrastructure security by McAfee and the Center for Strategic and International Studies (CSIS), nearly half of the respondents from the energy sector said they had found Stuxnet on their systems. Stuxnet has one intent: sabotage.

More recently, an apparent descendant of Stuxnet called Duqu has been reported in energy facilities in at least eight countries. Perhaps authored by the creators of Stuxnet, or at least using the older worm's source code, Duqu has not been used in any actual attacks to date – although it is capable of doing damage – but rather appears to be probing for sensitive information and weaknesses that could be exploited in future attacks.

While the physical destruction of facilities, with potentially deadly consequences, is a genuine concern, many cyberthreats are subtler in intent, seeking to gain sensitive intellectual property (a type of espionage) or to commit extortion. In fact, extortion is the most prevalent cyberthreat reported by the global energy sector. In the McAfee/CSIS study noted earlier, one in four power companies globally said they had been victims of extortion. In some countries, the incidence is alarmingly high: 80 percent in Mexico, for example, and 60 percent in India.

One of the challenges in confronting cyberthreats to the energy sector is that they take many forms, have disparate goals, and originate with a variety of sources, making it difficult to know which systems are at risk, which require protection, at what level, and at what cost.

Vulnerabilities of Energy Systems

The increased vulnerability of the energy sector is due, ironically, to well-intentioned efforts to modernize energy distribution. Energy system operators have historically been concerned with three technology domains: the industrial control systems (ICS) that run turbines, generators and other heavy-duty equipment; the system control and data acquisition, or SCADA, systems that oversee the ICS. SCADA systems don't actually run equipment but enable operational teams to monitor and manage the ICS through consoles known as "human-machine interfaces," or HMI. The third domain is the provider's organizational IT network—its internal databases and business applications.

In the past, these three domains operated separately, which of course was inefficient. As companies became more networked, they began automating the delivery of data across domains – which is useful but also means that an intruder could gain access to all three domains by entering just one of them. Add to this the fact that 70% of the energy grid is more than 30 years old, and the fact that workers can now reprogram systems through their smartphones – meaning the Internet – and you have quite a few points of vulnerability.

One area of vulnerability is in systems that are connected to the Internet and that also connect to non-cyber components. In this situation malicious instructions from the Internet can initiate actions on machines that connect to physical/kinetic infrastructure. This vulnerability occurs in systems where the monitoring systems connect to the physical systems via the Internet for remote access, efficiency and convenience.

Another area of vulnerability is, of course, from destructive malware: malicious instructions being introduced to a network via Internet files, USB drives, or other access. The malware itself can cause mass outages.

It's also worth noting that the threat landscape is not limited to cyber intrusions per se; people can use cyber tools to do the damage themselves. Witness the recent bank heists via ATMs. In this case, people hacked a database to harvest credentials, getting access to usernames and passwords so they could then get access to physical systems. The "cyber event" was a database intrusion, and the actions that followed were carried out by people. Just as people used fake ATM cards to rob the AT machines, people could also use illegally obtained credentials to cause harm to energy infrastructure that is controlled by computer access.

The Path Forward: Existing Regulation Must Become More Flexible

The good news is that both government and industry are well aware of these vulnerabilities and realize how important it is to protect the grid. The energy sector is highly regulated regarding cyber security, and operators must meet certain prescribed critical infrastructure protection (CIP) requirements. On the face of it, having CIP requirements sounds helpful. In practice, however, the regulatory process gets in the way of what started out as a good idea, making it, in practice, not helpful and maybe even harmful. McAfee has firsthand experience with this situation.

Two years ago some of our large energy customers came to us saying that that one of the CIP requirements seemed to mandate anti-virus protection to the exclusion of other, more modern, types of defenses. A/V is based on the concept of blacklisting, which creates a static list of what code will not be allowed into a system. In a dynamic threat landscape, however, the black list loses its accuracy in milliseconds. It both includes innocents and fails to block some recently turned bad actors. Blacklisting leads to a false positive rate and lack of detection that is not conducive to cyber security or network performance.

Whitelisting, on the other hand, fixes the false positive issues and allows for the fact that the adversary will penetrate any security walls we try to build. In concept, a "white list" is a list of *always accepted* actors, excluding other attempted entrants, thus eliminating the need to know if they cause harm. This can apply to IP addresses at the network layer or, as McAfee has implemented it for critical infrastructure, instructions at the kernel level of the operating system. This latter case is a nice fit for components with well-defined functionality that can be bounded with a white list approach, such as electric meters, other critical infrastructure components or ATM machines. There is a finite set of instructions that should ever run on such devices. Those instructions are on a "white list," and nothing else is permitted to execute on those devices, even if it penetrates the other security and enters the device. The instruction itself is worthless if it is not whitelisted.

Returning to the regulatory situation, once our customers pointed it out, we noticed that the CIP requirement did indeed seem to mandate A/V, or blacklisting. This meant that if an operator were to implement whitelisting, they could be in violation of the rule. The operator could file for a Technical Feasibility Exception, but absent that they would be faced with a violation. They were thus forced between being compliant and being secure – exactly the wrong result in the view of both government and industry. We brought this situation to the attention of energy regulators, who sympathized with the concern. However, getting the language changed would have required a process in which none of our customers cared to engage, so the rule still stands.

Now, a year and a half later, that old rule is due to be supplanted by a new rule that is technology-neutral and does not present a problem. That new rule is just in the comment phase, however, and will most likely not become effective until 2015. In this case the regulatory process, while well intended, is slow, cumbersome and – worst of all – dangerous, leaving a critical infrastructure without the latest cyber security technology.

Contrast this to our cyber enemies, who innovate swiftly and execute at the speed of light. By the time this rule is changed, our enemies will have moved onto something different. Innovation from the private sector can move along swiftly as well – if the regulatory process allows it.

For sectors such as energy, which are subject to cyber regulation, we urge the adoption of a faster review process, possibly an annual review of the rules. Any standard should be oriented towards outcomes rather than being prescriptive. The aim should be to give affected industries the ability to mix and match technologies to achieve the outcomes sought by regulators. Such an approach would also help promote security – and resilience – in situations where firms within an industry are different and have different organizational and security challenges.

For sectors that are not regulated, we believe that information sharing, industry innovation and positive incentives are what's needed.

Security Solutions

Information Sharing

Information sharing between the government and the private sector – and between private sector entities themselves – can be a powerful tool to thwart cyber adversaries. We commend NIST and DHS for the information sharing efforts they have initiated and fully support that processes each has begun. By information I mean not just general facts about threats but real-time malicious code that's being observed in systems around the world that can be shared instantaneously with global experts so that people and systems can act upon that information immediately. The financial services sector is particularly good at doing this through the FS Information Sharing and Analysis Center (ISAC), and other sectors have set up ISACs as well. But the information sharing process is not nearly as robust as it could be, mainly because private entities know they could incur liabilities.

The Rogers/Ruppersberger Bill

During the last Congress and again this year, your colleague on this committee, House Intelligence Committee Chairman Mike Rogers (R-Michigan), along with his Ranking Member Dutch Ruppersberger (D-Maryland), introduced the *Cyber Intelligence Sharing and Protection Act,* or CISPA. The House has once again passed the bill.

CISPA 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 voluntarily share information with the government.

The reason this is so important is that leading information technology companies, security providers and their customers are uniquely positioned to act as early warning systems that can identify and help address attacks on a real time basis, including APTs, botnets and other incursions. But under current law these private sector actors can't share the information needed to effectively combat these threats. Better enabling information sharing, including liability protections for private entities sharing cyber threat information in good faith, will help the private sector execute with the alacrity shown by our cyber adversaries and will enhance the public-private partnership that is so vital to meeting the cyber security challenge.

Ensuring that sufficient privacy protections are part of any information-sharing bill will help cement the broad consensus necessary to enact this proposal. Although the privacy and civil liberties improvements in the version of CISPA the House recently passed are significant, we would urge the sponsors to continue the ongoing dialogue with the privacy and civil liberties communities to address any remaining legitimate policy concerns.

Security Solutions – Innovation

The private sector is embracing innovation to constantly improve our capabilities to be resilient and challenge ourselves across industry, government, and owners of critical infrastructure. This is how we plan to win back the agility now enjoyed by the adversary. As mentioned earlier NIST is enabling innovation through partnerships with industry, and we applaud their efforts.

At McAfee we believe in a connected, adaptable, open and dynamic security platform to guide security decisions made by machines and people. We emphasize the importance of every network component being both a producer and consumer of intelligence. This intelligence can then be shared within the network and externally (as allowed by policy) to enable an adaptive, learning ecosystem that gets smarter as it protects.

This ecosystem concept is well described in the white paper from the National Protection and Programs Directorate within the Department of Homeland Security. Done correctly, networks can detect behaviors over time and begin to recognize, almost biologically, threats before those threats can overtake network functionality. Maturity models have shown that for any size organization, a wise design up-front leads to increasing security and decreasing cost over time. This ecosystem model would work well for the energy sector

We call this dynamic, comprehensive and open platform Security Connected.
Such a platform can enable any entity, any product, any utility, and any company small or large, to become part of a greater system where the detection of a threat on the Internet is used as protection going forward – at the speed of light. This is the agility our adversaries cannot achieve.

Security Solutions – Positive Incentives

As a front-line organization on cyber security, we know that innovation and cooperation between government and industry is vital. And the best way to get cooperation is with positive incentives, not more regulations. Congress must provide the necessary tools and assurances we need to lock down our nation's critical infrastructures. Steps that can be taken now include:

- Establishing cybersecurity as a national priority with funding for research and development, scholarships, competitions and other incentives to create a new generation of cybersecurity career professionals.

- Tax incentives to encourage businesses to invest in cyberdefense, including accelerated depreciation schedules or tax credits for adopting proven security technologies.

- Liability protections for companies that share information about malicious network intrusions with the government. Right now, liability fears can suppress timely sharing of vital threat data. Liability protections should also be available

for companies that use vetted technologies and services to protect themselves from cyber attacks. No legislation is needed to achieve this goal – simply encouraging the Department of Homeland Security to take the lead use its existing authority under the *SAFETY Act*, which provides liability protections to sellers and users of DHS reviewed and approved cyber security tools.

- Insurance reforms: Government could enhance the insurance market by providing it with a backstop program. To that end, Congress should consider extending the reach of the *Terrorism Reinsurance Program Reauthorization Act* (or TRIPRA) to include cyber attacks.

Thank you for requesting McAfee's views on these important issues. I am happy to answer any questions.