Testimony of

Dr. Phyllis Schneck
Vice President, Threat Intelligence, McAfee Corporation

On Behalf of the
Business Software Alliance

Before the

Subcommittee on Technology and Innovation
Committee on Science and Technology
United States House of Representatives

Hearing on

"Cybersecurity Activities at NIST's Information Technology Laboratory"

October 22, 2009

Chairman Wu, Ranking Member Smith, members of the Committee, thank you for the opportunity to testify today on the important issue of cyber security, and the role of the National Institute of Standards and Technology (NIST)'s Information Technology Laboratory (ITL.)

My name is Phyllis Schneck, and I am the Vice President of Threat Intelligence at McAfee. McAfee is the world's largest dedicated security technology company. McAfee is committed to relentlessly tackling the world's toughest security challenges. The company 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, browse and shop the web more securely.

As Vice President of Threat Intelligence, I am responsible for the design and application of McAfee's Internet reputation intelligence, strategic thought leadership around technology and policy in cybersecurity, and leading McAfee initiatives in critical infrastructure protection and cross-sector cybersecurity.

I testify today on behalf of the Business Software Alliance (BSA), of which McAfee is a member. BSA is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry and its hardware partners before governments and in the international marketplace.[1]

My testimony will address three questions:

1. What could NIST do to address some of the recommendations of the Cyberspace Policy Review?
2. What is our assessment of the proposed reorganization of NIST's ITL, and how will it improve the outcomes of ITL activities?
3. Given the current emphasis on information assurance and cyber security, what recommendations do we have on how ITL might improve its effectiveness or expand the scope of its activities and their impact?

1. What could NIST do to address some of the recommendations of the Cyberspace Policy Review?

McAfee and BSA welcomed the 60-day review ordered by the President. We believe that cyber security needs to be elevated as a priority of this country. We also welcomed the openness of the review process, which allowed a wide range of

[1] BSA members include Adobe, Apple, Autodesk, Bentley Systems, CA, Cadence Design Systems, Cisco Systems, Corel, CyberLink, Dassault Systèmes SolidWorks Corporation, Dell, Embarcadero, HP, IBM, Intel, Intuit, McAfee, Microsoft, Minitab, Quark, Quest Software, Rosetta stone, SAP, Siemens, Sybase, Symantec, Synopsys, and The MathWorks.

stakeholders, and in particular owners and operators of critical cyber infrastructure, to provide their views and recommendations. In the end, while the final report contains many recommendations and so will require that industry remain engaged throughout their implementation, McAfee and BSA were broadly supportive of the Cyberspace Policy Review's conclusions.

I would like to touch on a few of the recommendations of the Cyberspace Policy Review that we believe are of particular importance and relevance to NIST.

Firstly, we strongly support the Cyberspace Policy Review's call for an integrated US government strategy to influence the development of international standards on cyber security.

Such a strategy would recognize the important links between innovation, cyber security and international standards.

We believe innovation is key to greater cyber security. Those persons intent on doing harm, whether profit-motivated cyber criminals, cyber spies, hostile nations or terrorist groups, find new ways to attack and adopt new technologies all the time. We must stay a step ahead of them. To do this, innovation is key.

A necessary element of ensuring continued innovation is sound standards policy. Global, industry-led, voluntary standards and best practices create the environment where multiple innovative solutions can flourish by:

- Facilitating interoperability between systems built by different vendors.
- Facilitating competition between vendors, leading to greater choice and lower cost.
- Spurring the development and use of innovative and secure technologies, because industry-led standards are regularly updated.

This is why we urge the U.S. government to support and uphold global, industry-led standards and best practices on cyber security, by doing the following:

- First, the U.S. government needs to develop a comprehensive international cyber security standards strategy. What we have currently is a collection of ad hoc, incomplete and uncoordinated efforts. The White House Cyberspace Policy Review recognized this lack of coordination. NIST should play an important role in the creation and implementation of such a strategy. The strategy needs to answer the following questions:
    1. What cyber security standard development efforts is the U.S. currently involved in?
    2. What cyber security standards do we need?
    3. Where are they being developed?
    4. What agencies will represent the U.S. for each of them?
- Second, the government should identify the relevant international industry-led cyber security best practices, and recognize and promote their use in

federal systems. Government, industry and academia should collaborate to identify international industry-led best practices, and McAfee and BSA would eagerly contribute to such a process.

But there are also missteps the government should avoid. Most importantly, the government should not impose country-specific technology standards for cyber security, in particular standards developed by government agencies, except in narrowly tailored national security situations. This would set a precedent that other nations would follow to create their own, divergent standards. The end result would be at odds with the global nature of the Internet, would contribute to breaking up the global marketplace into national markets, and would inhibit rather than promote interoperability.

Finally, I would add that if NIST were tasked with creating and mandating such domestic standards, it would lessen the high regard it enjoys not just in the United States, but also internationally, as an arbiter of a process grounded in science.

Therefore, cyber security policymakers should support the global nature of the IT marketplace, rather than contribute to breaking it up into national markets.

We believe our position is fully consistent with President Obama's statement, when he released the Cyberspace Policy Review on May 29: "*My administration will not dictate security standards for private companies. On the contrary, we will collaborate with industry to find technology solutions that ensure our security and promote prosperity.*"

<u>Secondly, I would like to say a few words about the Cyberspace Policy Review's recommendation to launch a public education and awareness campaign.</u>

Educating the public about threats and about common sense measures it can adopt to protect itself, is important. That is why the CEOs of BSA raised this issue when they met with Secretary of Homeland security Napolitano this year. Many BSA members, including McAfee, have made important investments in educating the public about cyber security, for example by actively supporting and sponsoring the National Cyber Security Alliance (NCSA), the preeminent public-private partnership between industry, the U.S. Department of Homeland Security (DHS) and non-profit institutions, to promote cyber security awareness for home users, small and medium size businesses, and primary and secondary education.

McAfee and BSA believe a major education and awareness campaign on the scale envisaged by the Cyberspace Policy Review should build upon the foundation of the NCSA. If NIST were to take a role in education and awareness, we recommend that it do so through the national campaign that NCSA should coordinate. NCSA should be the focal point, using and expanding the relationships and brand it has already built with a multitude of local stakeholders – schools and universities, community-based

organizations, local governments, local chambers of commerce, home-owners associations, etc.

Thirdly, NIST has a valuable role to play in carrying out the Cyberspace Policy Review's call for building a cybersecurity-based identity management vision and strategy.

Identity and authentication are foundational building blocks of a modern and fundamentally secure cyber space. The Administration is already working to implement this recommendation of the Cyberspace Policy Review, and we expect them to issue a draft document in the coming months to the public for comment.

NIST should play a critical role in crafting and implementing this government strategy, on the basis of the important contributions it has made to previous federal identity and authentication initiatives, such as the implementation of Homeland Security Presidential Directive 12 (HSPD-12.) As identity and authentication can apply not only for individuals, but also for devices, NIST's ability to advise and influence this strategy will be critical to ensuring its technical feasibility and operational success.

As the Cyberspace Policy Review notes, it is important that the government not mandate the use of specific identity management systems, but rather ensure that they are available as opt-ins. We also agree with the Review that a variety of interoperable systems should be offered, rather than the government picking a single provider or technology, which would stifle innovation.

2. **What is our assessment of the proposed reorganization of NIST's ITL, and how will it improve the outcomes of ITL activities?**

BSA has not had the opportunity to reach a common position among its members on the reorganization of the ITL. However, I would like to make the following comments about what is at stake.

First, we believe two important factors in the future success of the Computer Security Division (CSD) of the ITL are budget and manpower. CSD is already under-resourced and under-staffed. As we give them new missions in a context of tighter federal budgets, sufficiency of resources will be a key concern. We will also need to ensure that NIST funds intended by Congress for cyber security are not spent on other projects, and this can be achieved by requiring that ITL regularly report to this Committee on how it spends funds designated for cyber security.

Second, the process that will determine the future course of the ITL needs to be open, transparent and based on the input of the wide range of stakeholders, in particular from the IT industry and academia, who work with CSD.

And third, the guiding principle should be to avoid diminishing the visibility, priority, and resources accorded to cyber security within NIST.

3. **Given the current emphasis on information assurance and cyber security, what recommendations do you have on how ITL might improve its effectiveness or expand the scope of its activities and their impact?**

First, McAfee and BSA want to restate their deep appreciation for the outstanding work done by the ITL and CSD over the years.

I would like to highlight two reasons in particular that have contributed to establishing ITL as a widely-respected leader:

1. ITL works collaboratively with stakeholders. Its work products are well regarded because they draw upon the best contributions of leading experts in their fields, from industry but also from academia. One of the most salient examples is the AES encryption standard, whose underlying cryptographic algorithm had been developed by Belgian academics and selected through a rigorous competition. The openness of the selection process has greatly contributed to inspiring confidence in AES and thus in its wide adoption outside the federal government.
2. For the security of federal systems, and with very few exceptions, ITL does not in fact enact mandatory technology standards. Rather, it offers guidance – through its Special Publications 800 (SP 800) series – that are flexible enough to allow each agency to adopt the security posture most appropriate to its risk profile. We need to ensure that federal agencies more consistently implement this guidance.

As Congress considers how to reform FISMA to place greater emphasis on actual security of federal networks and systems, federal agencies will need in particular that CSD expand its scope of activities, building on its legacy of public-private collaboration and non-mandatory guidance, to produce the following:

- Government-wide standards and guidelines for real-time monitoring, auditing and analysis of data about the security, performance and health of federal networks and systems across the entire federal government. This would contribute to providing holistic, end-to-end security of federal networks, rather than focusing on the security of single points of failure.
- Government-wide standards and guidelines for sharing threat and vulnerability information among federal agencies and with the private sector. While we think, as I said before, that NIST should always work collaboratively with stakeholders, given the private sector impact of information sharing, any NIST effort in this area should be undertaken jointly with the private sector, in coordination with DHS.

Global, industry-led standards must continue to underpin the global IT ecosystem. Therefore, these two categories of NIST standards and guidelines should draw from global, industry-led standards to the greatest extent possible.

Importantly, in producing such standards and guidelines, NIST should spur innovation by always striving to, per the terms of the National Institute of Standards and Technology Act, "*ensure that such standards and guidelines do not require specific technological solutions or products, including any specific hardware or software security solutions; ensure that such standards and guidelines provide for sufficient flexibility to permit alternative solutions to provide equivalent levels of protection for identified information security risks; and use flexible, performance-based standards and guidelines that, to the greatest extent possible, permit the use of off-the-shelf commercially developed information security products.*"[2]

Finally, NIST must continue to push at the edges of cyber security research and development. BSA has expressed in the past to this committee the importance that we attach to research and development (R&D) to improve our nation's cyber security, and we have called for a national cyber security R&D plan. We believe that NIST would play an important role under such a plan, given its own R&D work and its ability to reach out to the R&D arms of many companies.

In conclusion, I want to reiterate the importance that we attach to:

- Innovation as a major tool to improve our cyber security;
- The role that R&D and international, industry-led standards play in spurring innovation and in improving cyber security; and
- The development by the U.S. government of an international cyber security standards strategy.

[2] Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g–3), subsection (c)(5-7).