Statement for the Record
Dr. Mark Bregman
Chief Technology Officer
Symantec Corporation
Before the
United States House of Representatives
Committee on Science and Technology
Subcommittee on Technology and Innovation
June 25, 2009

Good afternoon, Chairman Wu, Ranking Member Smith and Members of the Subcommittee on Technology and Innovation. Thank you for the opportunity to speak about cybersecurity activities at NIST and DHS.

I come before you today as Chief Technology Officer of Symantec Corporation, the global leader in providing information security solutions. We protect consumers and businesses by assuring the security, availability and integrity of their information. Headquartered in Cupertino, California, Symantec is the world's fourth largest software company with operations in more than 40 countries and over 18,000 employees.

In April, Symantec released our Internet Security Threat Report which is widely acknowledged to be the most comprehensive analysis of information security activity for today's economy. The Report includes an analysis of network based attacks including those on small businesses with a review of known threats, vulnerabilities, and security risks. Symantec has provided this Report since 2002.

This year's report showed that the cyber attacks are growing in size, scope and sophistication. They are becoming more targeted and more dangerous to our critical infrastructure on which our economy depends. Vulnerabilities also continue to increase dramatically.

The most common type of attack this period targeting government and critical infrastructure organizations was denial-of-service attacks, accounting for 49 percent of the top 10 in 2008. Denial of Service (DoS) attacks are a threat to government and critical infrastructures since the purpose of such attacks is to disrupt the availability of high-profile websites or other network services and make them inaccessible to users and employees. This could result in the disruption of internal and external communications, making it practically impossible for employees and users to access potentially critical information. Because these attacks often receive greater exposure than those that take a single user offline, especially for high-profile government websites, they could also result in damage to the organization's reputation. A successful DoS attack on a government network could also severely undermine confidence in government competence, and impair the defense and protection of government networks.

DoS attacks can often be associated with political protests, since they are intended to render a site inaccessible in the same way that a physical protest attempts to block access

to a service or location. They can also be associated with conflict whereby one country may attempt to block Web traffic or take websites offline. As such, the high percentage of DoS attacks may be an attempt to express disagreement with targeted organization or countries. Examples of these types of attacks targeting governments were the DoS attacks that disrupted and took Estonian governmental websites offline in 2007 and the Georgia government websites that were rendered inaccessible during the Georgia-Russia conflict in 2008.

SMTP, or simple mail transfer protocol, is designed to facilitate the delivery of email messages across the Internet. Email servers using SMTP as a service are likely targeted by attackers because external access is required to deliver email. In addition to illegally accessing networks, attackers who compromise email servers may also be attempting to use the email servers to send spam or harvest email addresses for targeted phishing attacks. Because spam can often consume high quantities of unauthorized network bandwidth, these emails can disrupt or overwhelm email services, which could result in DoS conditions. Successful SMTP attacks against government and critical infrastructure organizations could also allow attackers to spoof official government communications and obtain credentials in order to launch further attacks. These organizations heavily rely on email as a communication method and as such, it is essential that email traffic be secured. This is just one example of the type of threat affecting government and critical infrastructure sectors in cyberspace today.

As the President so eloquently articulated in May when he released the 60 day cyber review,

"The globally-interconnected digital information and communications infrastructure known as "cyberspace" underpins almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety and national security." The report goes on to say "Cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century".

We applaud the President's personal commitment to take the action that is so desperately needed around cybersecurity and look forward to working soon with the new cyber security coordinator, other agencies and stakeholders to develop the strategy, policies, and operational plans necessary to improve cyber security. We hope that the coordinator will be elevated within the White House and have the appropriate policy, decision-making and budget review authorities necessary to set the strategic direction for the nation, empower agencies and the private sector to do their mission in a coordinated and balanced way, and take a more prominent role in international cyber policy.

Cyber Security: A Shared Public and Private Sector Responsibility

Cybersecurity isn't a civilian or military problem, or even a government problem -- it's a universal problem. All networks, military, government, civilian and commercial, use the same computers, the same networking hardware, the same Internet protocols and the same software packages. We all are the targets of the same attack tools and tactics. It's

not even that government targets are somehow even more differentiated; these days, most of our nation's critical IT infrastructure is in commercial hands. Government-sponsored or civilian hackers go after both military and civilian targets.

GAO reports indicate that government problems include insufficient access controls, a lack of encryption where necessary, poor network management, failure to install patches, inadequate audit procedures, and incomplete or ineffective information security programs. These aren't top security issues; these are the same managerial problems that every corporate CIO wrestles with.

We all have the same information security challenges, so solutions must be shared. If the government has any innovative ideas to solve its cybersecurity problems, certainly a lot of us could benefit from those solutions. In addition, we need transparent and accountable government processes, using commercial security products. Finally, we also need government cybersecurity programs that improve security for everyone.

Now, I will keep the remainder of my comments focused on what DHS and NIST's respective roles and responsibilities are or should be in cyberspace.

DHS' Cyber Roles and Responsibilities

Let me start with the Department of Homeland Security or "DHS". Under the National Infrastructure Protection Plan construct, DHS is the lead department for engaging with the IT Sector. In addition to the 60 day rollout, there has been a lot of talk regarding the "Comprehensive National Cyber Initiative" or "CNCI". Symantec and other private sector stakeholders, through the Sector Coordinating Councils, have been able to participate and provide input into DHS on a number of the Initiative's projects, including Project 12 regarding public-private partnerships, Project 4 on leap ahead technologies, and Project 10 on deterrence and the need for global norms of behavior in cyberspace. The private sector and DHS have been in engaged in a number of other projects and activities to address a myriad of cyber policy issues, including resiliency, incentives, metrics, risk assessments, information sharing, and cyber exercises just to name a few. We have seen a marked improvement over the last couple of years by the DHS and their engagement with the private sector.

There are a few areas we believe more can be done by the Department of Homeland Security and private sector jointly. As you heard from Dr. Fonash last week, there are three areas in which DHS has focused their priorities around CNCI: Establishing a front line of defense, seeking ways to defend against a full spectrum of threats through supply chain and intelligence, and taking cyber security to the next level through workforce education.

1) Front Line of Defense: In cyberspace we have a very rich, traditional base from the commercial sector very different from other historical government models for addressing national security issues where much of the solutions come from government or defense contractors. With that in mind, it could benefit the U.S. government greatly if the private

sector were brought in more consistently to assist in the development of cyber security solutions to address projects and other key cyber challenges. We would like to see more collaboration between the public and private sector on these programs so that the government can learn about what technologies may be more applicable now to address today or tomorrow's threats. One example of where more input from the private sector could be helpful is Project Einstein. Project Einstein was developed to detect network intrusions and create better situational awareness. However, since its inception a number of years ago, the threats and technologies used to prevent or mitigate against these threats have changed dramatically. No longer is delayed detection of threats and intrusions and delayed simply enough. The need for data prevention technologies and near or real-time situational awareness capabilities are imperative. We hope the public sector leverages the expertise and technology that the private

2) Supply Chain: In last week's hearing, there was a lot of discussion by the government witnesses on the importance of protecting our global supply chain. We heard about the work that the Department of Homeland Security and Department of Defense are undertaking to lead the CNCI Project on this topic. To date, the private sector has not been formally asked to participate in this activity despite the fact that much of the supply chain that government cares about is in the hands of the private sector. We as a company take actions on what we know and the risks we face. However, if more information is not shared by the government on the threats or risks they see, how can we do more to protect against the threats or risks that we have not been informed about? Additionally, we believe that much of the expertise and best practices for protecting supply chain reside within the private sector. Let me give you one example.

Symantec is a co-founder of SAFECODE, a non-profit organization created for companies to share software assurance and supply chain best practices. We strongly urge the Department of Homeland Security, Department of Defense, NIST and other agencies to work closely with SAFECODE and its member companies to work collaboratively in addressing supply chain and software assurance. This collaboration could focus on information sharing of supply chain threats and vulnerabilities and development of best practices and standards.

3) Education and Awareness: DHS has taken a lead role in this area. For example, DHS is a sponsor and active participant in the National Cyber Security Alliance (NCSA) and staysafeonline.gov. The purpose of NCSA, a 501c3, is to educate consumers, K-12, higher education, and small and medium sized businesses the steps they need to take in order to use the Internet safety and securely, protecting themselves, their data and the cyber infrastructure. The President's 60 day cyber review recognized the good work of the NCSA and highlights the need for formal K-12 education and curriculum to address cyber safety, cyber security and cyber ethics (C3) within schools. NCSA ad DHS will be working with other key stakeholders to develop this C3 framework. In addition to a K-12 curriculum framework, NCSA has established a volunteer program (C-SAVE) for computer security professionals to teach cyber security in schools and is working to conduct a small and medium-sized business study to identify current cyber practices, gaps, resource needs, and ways to effectively communicate with this important audience.

There are many more activities underway which can be found at www.staysafeonline.gov.

4) Workforce and training: In addition to education and awareness responsibilities, DHS is working with several agencies, NCSA and other stakeholders to develop a plan for the development and retention of a trained cyber security professional workforce that can meet the increasing demand and gaps within the government. DHS is also developing a program to retrain the current workforce in the public and private sector to ensure they have the most up-to-date skills and capabilities to address today's technology and cyber security demands. We fully support these activities and believe this appropriate work for DHS to engage in with other interagency partners.

5) Exercises and national incident response planning: The 60 day review's near-term action plan calls for "a cyber security incident response plan to enhance public-private partnerships with an eye toward streamlining, aligning, and providing resources to optimize contribution and engagement". We believe that DHS is well positioned to help lead these efforts and ask that the private sector be included early on in the development process.

6) R&D: DHS has a role to play in the area of cyber security R&D through the Science and Technology Directorate. The S&T Directorate maps their R&D projects based on the needs of their primary internal customer, the Cyber Security and Communications Directorate. We believe that much of the work completed by the S&T directorate is very important and believe that increased funding is necessary in order for the S&T Directorate to meet their customers' needs. We also believe that a more formal process of identifying priorities and coordinating with internal customers is necessary. We also believe that DHS writ large, in their capacity as the Government Specific Agency for interacting with the IT and Communications Sectors, must have a formal process of engaging with the private sector on the CNCI R&D Project. It is not surprising that the private sector spends more than the U.S. government on R&D. It is also not surprising that both the public and private sector have limited resources with which to spend on R&D.

Imagine if we could work together to identify what the collective problems and priorities are for government and industry, determine which of those priorities are commercially viable and therefore should not be funded by government, and identify the gaps and/or redundancies that exist. Those projects which may be redundant can be deconflicted and reallocated. Those priorities that are gaps and not determined to be commercially viable could then be funded by government. This process would allow us all to maximize our collective resources to the fullest extent possible and ensure that we are working from a coordinated roadmap and set of priorities. We respectfully ask that the U.S. government engage with the private sector to the extent possible in this area. Some initial challenges or problem areas for R&D consideration could include: Attribution, Situational Awareness, Early Warning, and ID management.

NIST's Roles and Responsibilities

In addition to DHS' role, NIST's mission in cyber security is very important. Beginning with its founding in 1901 as the National Bureau of Standards, NIST has played a key role in US commerce through promotion of various national standards. In particular, the work NIST does with federal agencies, industry and academia to research, develop and deploy information security standards and technology is critical. As cyber security standards and metrics become increasingly important, NIST's role and responsibility will continue to grow. With that, we believe NIST's funding level is not adequate and should increase so they can meet the community's growing needs and requirements.

FISMA: Since its inception, NIST has played a leading role in the development of FISMA guidelines and Federal Information Processing Standards (FIPS). As Congress looks to reform FISMA, we will look to NIST for appropriate guidance and standards.

Common Criteria/ NIAP and other international standards activities: Symantec has been involved with Common Criteria evaluations for several years. In fact, our Symantec Enterprise Firewall was the first product to be certified against the US Government's application firewall protection profile. We currently have several products currently certified. Symantec supports the Common Criteria because it offers many advantages, including an international certification framework for products. Based on the results of evaluations against the Basic and Medium Robustness Protection Profiles and comments from vendors and government customers, NIAP, the U.S. government implementation arm for Common Criteria, has determined that the current U.S. Protection Profile Robustness model needs to be revised. The original implementation did not create the necessary test plans and documentation needed to achieve consistent results across different products evaluated in different labs. As a result, NSA is creating a Standard Protection Profile, which will replace any corresponding U.S. Government Protection Profile. NSA plans to work with industry, government stakeholders, and the Common Criteria community to create these Protection Profiles. As the lead technical standards organization for the federal government, we believe that NIST has a critical role to play in revising the protection profiles and improving Common Criteria. We ask that NIST become an active member of NIAP again and would like to see them play an even more active role in other international consensus standards bodies and organizations.

Flexible NIST Federal Security Standards: NIST has contributed to raising the quality of federal information security by promoting operational norms and by helping agencies to find model security processes. Experience shows that federal standards aligned with established commercial practices generally succeed. However, unique government-only standards, such as the Government Open Systems Interconnection Profile (GOSIP), have achieved poor results.

Whether flexible or rigid, standards must be appropriate for the activities being regulated, and they must be mindful of market drivers and required precision. The precision and specificity in standards vary considerably according to their goals and purposes. For

example, some technical standards, such as communications protocols, must be very precise and rigid because of a need for interoperation among many vendors' products.

Thus, credible federal mandates must strike a balance between ideal and practical standards, including setting realistic expectations for compliance in the huge base of installed federal systems. Additionally, we must remember that compliance will be put in jeopardy if the standards are perceived to be unreasonable or not viable.

First, standards require reliable metrics to enable tracking of compliance. Second, they must be introduced at a specific point in the product life cycle when customers seek standard products and manufacturers are no longer competing on features. Third, there must be a compelling market benefit supporting use of a standard. Finally, standards must be appropriate for the application being standardized.

NIST's guidelines strike a balance between general rules of thumb for all agencies and the local knowledge and expertise of on-the-ground federal officials. However, fixed, inflexible process standards cannot easily accommodate all of these situations. In summary, the constant changing cyber threat landscape and its high reliance on human activity coupled with the rapid changes in technology make it essential that security doctrine remains flexible.

Metrics: The Near-term action plan within the President’s cyber review requires the establishment of cyber security performance metrics. This is an area ripe with opportunity and we believe NIST should be a key driver of this activity working with the private sector and other agencies.

In addition to cyber security metrics, there are some areas we believe NIST should consider collaborating more with the private sector on, including: Cloud Computing architecture and standards, SCAP and other data taxonomy standards, Supply Chain best practices, Health IT, and Smart Grid architecture with security standards built in. We also want to stress the importance of NIST and OMB working with the private sector to ensure that agreed upon standards, protocols and requirements are rolled out with the reasonable timelines and milestones to meet realistic commercial product development roadmaps.

In conclusion, we believe both the Department of Homeland Security and NIST have done much to carry the cyber torch forward in several areas. However, there is much more work to be done and much more collaboration that needs to take place with the private sector. We stand committed to working with the Administration and Congress to improve cyber security.

Thank you again, Chairman Wu, for allowing me the opportunity to testify before the distinguished members of the House Science Subcommittee on Technology and Innovation regarding Cyber security responsibilities for DHS and NIST. I am happy to answer any questions that any members of the Committee may have.