Cybersecurity: Preventing Terrorist Attacks and Protecting Privacy in Cyberspace

Testimony of the
National Security Agency's Information Assurance Director
Before the Senate Committee on the Judiciary's Subcommittee
On Terrorism and Homeland Security

Statement for the Record

November 17, 2009

Good morning, Chairman Cardin, Ranking Member Kyl, and distinguished members of the Subcommittee. My name is Richard C. Schaeffer, Jr., and I am the National Security Agency's (NSA) Information Assurance Director. I appreciate the opportunity to be here today to talk briefly about the NSA's information assurance mission and its relationship to the work of the Department of Homeland Security and others concerned with helping operators of crucial information systems protect and defend their data, systems and networks from hostile acts or other disruptive events.

I would also like to thank the Chairman and the other members of the Subcommittee for their continued interest in, and attention to, this issue. Each day, ever more data and functions that are vital to the nation are consigned to digital systems and complex, inter-dependent networks. There are no "silver bullets" when it comes to cybersecurity, but over time, increased awareness of cybersecurity issues, new standards, better education, expanded information sharing, more uniform practices, and improved technology can and does make a meaningful difference.

The NSA information assurance mission focuses on protecting what National Security Directive 42 defines as "national security systems", systems that process, store, and transmit classified information or are otherwise critical to military or intelligence activities. Historically, much of our work has been sponsored by and tailored for the Department of Defense. Today, national security systems are heavily dependent on commercial products and infrastructure, or interconnect with systems that are. This creates new and significant common ground between defense and broader U.S. Government and homeland security needs. More and more, we find that protecting national security systems demands teaming with public and private institutions to raise the information assurance level of products and services more broadly. If done correctly, this is a win-win situation that benefits the whole spectrum of information technology (IT) users, from warfighters and policymakers, to federal, state, local and tribal governments, to the operators of critical infrastructure and the nation's major arteries of commerce.

This convergence of interests has been underway for some time and we can already point to significant examples of the kind of fruitful collaboration it inspires. For instance, the NSA and the National Institute of Standards and Technology (NIST) have been working together for several years to characterize cyber vulnerabilities, threats, and countermeasures, to provide practical cryptographic and cyber security guidance to both

IT suppliers and consumers. Among other things, we've compiled and published security checklists for hardening computers against a variety of threats; we've shaped and promoted standards that enable information about computer vulnerabilities to be more easily cataloged and exchanged and, ultimately, the vulnerabilities themselves to be automatically patched; and we've begun studying how to extend our joint vulnerability management efforts to directly support compliance programs such as those associated with the Federal Information Security Management Act. All of this is unclassified and advances cyber security in general, from national security and other government networks to critical infrastructure and other commercial or private systems.

The NSA partners similarly with the Department of Homeland Security (DHS). Earlier this year we together proudly announced the designation of 29 additional U.S. colleges and universities as National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) and/or Information Assurance Research (CAE-R). This brings the number of institutions participating in this highly regarded program to 106, located in 37 states, the District of Columbia and the Commonwealth of Puerto Rico.

Universities designated as National Centers of Academic Excellence in Information Assurance are eligible to apply for scholarships and grants through both the Federal and Department of Defense Information Assurance Scholarship Programs. Graduates from Information Assurance programs at CAE institutions become a critical part of the core of professional cyber security experts protecting national security information systems, commercial networks and critical information infrastructure. These professionals are helping to meet the increasingly urgent needs of the U.S. government, industry, academia and research.

The NSA/DHS partnership was formed in 2004 in response to the ***President's National Strategy to Secure Cyberspace*** of 2003. The CAE-R program was added in 2007 to encourage universities and students to pursue research, development and innovation in Information Assurance (cyber security). The program originally created by this partnership has continued to grow and become even more relevant and critical to U.S. national security today.

NSA and DHS collaborate daily, cooperating on investigations and forensic analysis of cyber incidents and malicious software, and together we look for and mitigate the vulnerabilities in various technologies that would render them susceptible to similar attacks. We each bring to these efforts complementary experience, insight, and expertise based on the different problem sets and user communities on which we concentrate, and we each then carry back to those communities the dividends of our combined wisdom and resources.

Key to the Nation's Cybersecurity efforts is the Public-Private Sector relationship, which has been actively embraced by the Federal Government, industry and academia. This trusting relationship includes...and is based upon...the common goal of improving cybersecurity, the sharing of information, and collaborative research, development and innovation. A recent example of this continuing and close collaboration is last month's 5th Annual Security Automation Conference at the Baltimore Convention Center, co-

hosted by NSA, NIST, DHS and the Defense Information Systems Agency (DISA). In fact, it brought together for several days nearly 1,000 representatives from the public and private sectors and demonstrated the benefits of automation and standardization of vulnerability management, security management, and security compliance.

In the past, proprietary technologies and methodologies have made it difficult to identify, remediate, and report on vulnerabilities in mission critical systems and data. Over the past few years, the Information Assurance Directorate at NSA has played a leadership role in developing security automation standards and fostering the adoption of security automation and security baselines across the DoD. These standards include the Security Content Automation Protocol (SCAP), Common Vulnerability Enumeration (CVE) and the Federal Desktop Core Configuration (FDCC). This year's conference showcased numerous SCAP-validated tools designed to simplify security management in DoD systems, increase interoperability in products, and reduce the cost of vulnerability management for our DoD customers. Established by NIST five years ago with an attendance of less than 50 people, the conference is now jointly sponsored by the four agencies, mentioned above. The benefits reach throughout industry as evidenced by the major industry vendors who participated.

NSA works directly and indirectly with vendors across the information technology and security community to develop and distribute configuration guidance for a wide variety of software and hardware products. We engage vendor products through deep technical analysis of vulnerabilities within the technology and from what we learn by conducting operations to find vulnerabilities in DoD systems. NSA keeps abreast of new vulnerabilities in these technologies and strives to provide customers and the IT community with the best possible security options for the most widely used products across the IT community and the DoD.

NSA, in partnership with NIST, Mitre, Symantec, McAfee, Intel, and many other security vendors, is actively encouraging the IT industry to utilize SCAP Protocols to provide managers with a greater understanding of risks, real data upon which to make management decisions, and the ability to give technical direction regarding the security of their networks and applications. SCAP is a group of standards that enable organizations to automate compliance, manage vulnerabilities, perform security measurement, and perform a host of other Asset, Vulnerability, and Configuration Management related tasks. Further, NSA's technical expertise and operational knowledge in cryptography improves hash standards for commercial industry through NIST's Hash competition. NSA brings its experience to the NIST decision making process, which selects high assurance hashes that commercial industry uses to secure things such as the storage of passwords and to provide software integrity checks.

Starting in 2005, NSA started working with DISA, DHS, NIST, Microsoft, Army, Navy, Marines, and Air Force to build consensus on common security configurations for Microsoft Operating systems such as XP, Vista, Internet Explorer, and firewalls. These common configurations ensured improved security, performance, power management, feature compatibility, and usability configuration settings for DoD purchased systems.

The Air Force utilized these settings to develop the Federal Desktop Core Configuration (FDCC) for all Air Force purchased operating systems. Working with vendors to pre-configure, pre-install, and pre-test configurations of their OS helps reduce purchase costs, improve security, and enables improved vulnerability and situational awareness. This FDCC work, ultimately saving millions of dollars for DoD, led to OMB adoption of the Windows/IE configurations as Federal-wide standards. NSA and the configuration working groups are now engaging additional vendors such as Apple, Sun, and RedHat to develop secure baselines for their products.

The recent announcement by Microsoft of the release of Windows 7 was quickly followed by the release of the security configuration guide for this state of the art operating system. Working in partnership with Microsoft and elements of the DoD, NSA leveraged our unique expertise and operational knowledge of system threats and vulnerabilities to enhance Microsoft's operating system security guide without constraining the user's ability to perform their everyday tasks, whether those tasks are being performed in the public or private sector. All this was done in coordination with the product release, not months or years later during the product lifecycle. This will improve the adoption of the security advice, as it can be implemented during installation and then later managed through the emerging SCAP standards.

As LTG Alexander, NSA's Director, stated clearly in his address to the RSA Security Conference this past April, Cybersecurity is a big job and it's going to take a team to do it. We'll bring our technical expertise and working with many others in the public and private sector we'll comprise the "team" the nation needs to address this challenge.

This concludes my remarks. I would be pleased to answer questions from you and others members of the Subcommittee.