Cyber Security: Recovery and Reconstitution of Critical Networks

Testimony of the
National Security Agency's Information Assurance Director
Before the Senate Homeland Security and Government Affairs Subcommittee on Federal Financial Management, Government Information, and International Security

Statement for the Record

July 28, 2006

Good afternoon Mr. Chairman and distinguished members of the Subcommittee. I appreciate the opportunity to be here today to talk briefly about the National Security Agency'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 prepare for and recover 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 cyber security, but over time, increased awareness of cyber security issues, new standards, better education, expanded information sharing, more uniform practices, and improved technology can and do make a meaningful difference.

My name is Richard C. Schaeffer, Jr., and I am the NSA's Information Assurance Director. The NSA information assurance mission focuses on protecting, so-called,"national security information systems" that handle 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 though, national security systems often rely on commercial products or infrastructure, or interconnect with systems that do. 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 generally. 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, and local governments, to the operators of critical infrastructure and major arteries of commerce.

This convergence of interests has been underway for some time and we can already point to several 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 that harden 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). In 2004 DHS joined the NSA in sponsoring the National Centers of Academic Excellence Program to foster training and education programs to support the nation's cyber security needs and increase the efficiency of other Federal cyber security programs. As of June of this year, 75 such centers have been established across 32 states and the District of Columbia. The NSA also supplies trained personnel and other technical support to the U.S. Computer Emergency Readiness Team and other operational activities of the DHS National Cyber Security Division, and we routinely alert one another to possible or emerging hostile cyber acts. In fact, DHS has just named an integree to work in the NSA/CSS Threat Operations Center, an organization that monitors the operations of the global network in real time to identify network-based threats to DoD and Intelligence Community networks.

NSA and DHS also cooperate 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.

With regard to post-incident response, the NSA supplies technical personnel and advice to help the DHS Infrastructure Protection Division plan for the interoperable communications systems needed to support an efficient recovery. The NSA also maintains a stock of secure communications equipment to replace or augment deployed systems in the wake of emergencies or other urgent and unforeseen needs. Following Hurricane Katrina, for instance, the NSA supplied encryption devices, secure satellite telephones, and cryptographic keying material to many DoD and civil entities involved in rescue and recovery; we also helped the National Aeronautics and Space Administration (NASA) reestablish secure connectivity between the Stennis Space Center near Bay St. Louis, Mississippi, NASA headquarters in Washington, and NASA's Marshall Space Flight Center in Huntsville, Alabama. When it comes to reconstructing networks more generally, however (beyond just communications systems), bringing in replacement technology may be the easy part. The real challenge is knowing *what* to reconstruct. That means maintaining an up-to-date understanding of just what set of data, functions, and connections – available to what set of users – qualify as critical. It also requires regular mapping and analysis to track the shifting physical and logical make-up of these nets.

Looking forward, NSA and DHS interests will continue to merge and the opportunities – and need – for shared work and mutual support will continue to grow. As once unique environments such as national security systems, computerized industrial controls (i.e., supervisory control and data acquisition, or SCADA systems), emergency services communications, and specialized financial and logistical networks come to rely on the same commodity hardware and software and commercial infrastructure and services, we

find ourselves concerned with many of the same vulnerabilities, threats, and countermeasures. We both have a stake in expanding the market for secure information technology and in steadily raising the bar when it comes to defining what's secure and what isn't. We both have a responsibility to help IT suppliers improve their products and to help IT buyers and operators make more informed choices about what to buy and how to assemble, configure, run, monitor, and defend their systems. And, since none of this is possible without security-savvy IT professionals, information assurance education and training remains a joint imperative.

Finally, beyond technical convergence, in the post 9/11 world the NSA and DHS are also bound together by the need to provide for communications across once unbridgeable chasms of classification and practice, from the President all the way to first responders and the guardians of critical infrastructure. As a starting point, the NSA and NIST have established a suite of unclassified cryptographic standards that can be implemented in commercial-off-the-shelf offerings as well as specialized high-end government equipment. This sets the stage for interoperable encryption and message authentication and is an important step – although just one step -- in the broader effort to ensure that the nation can recognize and respond to impending emergencies or their aftermath.