National Security Agency

Statement by

Daniel G. Wolf

Director of Information Assurance

National Security Agency

Before The

House Select Committee on

Homeland Security

Subcommittee on

Cybersecurity, Science and Research & Development

Hearing on

"Cybersecurity—Getting it Right"

July 22, 2003

Thank you Chairman Thornberry and the members of the Subcommittee. I am honored to be here and pleased to have the opportunity to speak with your committee to discuss cybersecurity research from the point of view of the National Security Agency as we conduct our mission to address threats to the security of critical U.S. Government information systems.

I also would like to thank the Chairman and other members of the Subcommittee for their strong interest and attention to this vital area. In my opinion, your leadership is important for raising awareness of the serious security challenges we all face in our age of interconnected, inter-dependent digital information networks.

My Name is Daniel Wolf and I am NSA's Information Assurance Director. NSA's Information Assurance Directorate is responsible for providing information assurance technologies, services, processes and policies that protect national security information systems. We are also responsible for conducting the research and development of information assurance technologies and systems.

I would like to note that NSA's Information Assurance Directorate and its predecessor organizations have had technical and policymaking responsibility regarding the protection of national security telecommunications and information processing systems across the Executive Branch since 1953.

In regards to your theme for this hearing: "Cybersecurity—Getting It Right." I am not sure that NSA has all of the answers or that we always have gotten it right—but I am quite confident that during our 50 years of deploying communications and now cyber security products we have learned quite a few lessons. We have had tremendous successes and our share of failures. We also have gained a deep understanding and respect for the challenges the nation must overcome to begin to tame cyberspace.

Some in government and industry want to keep NSA in a box labeled "for classified information only." They suggest that NSA's perspective is much too narrow due to our focus on the stringent requirements of national security systems. However, I

believe quite the contrary. It has been my experience—and my testimony will soon address—that there is little difference between the cybersecurity that is required for a system processing top-secret military information and one that controls a segment of the nation's critical infrastructure.

Both systems require the element of assurance or trust. Trust that the system was designed properly. Trust that it was independently evaluated against a prescribed set of explicit security standards. Trust that it will maintain proper operation during its lifetime, even in the face of malicious attacks and human error. It has been my experience that effective cybersecurity must be baked into information systems starting at the R & D phase. Trust cannot be sprinkled over a system after it is fielded.

Homeland security presents another reason to suggest that cybersecurity requirements must converge. The information management principle within the national security community has always been the concept of need-to-know. But the fundamental information principle for homeland security is need-to-share. With need-to-share we must develop technical solutions for secure interoperability that may be called on to tie top-secret intelligence systems to a local first responder system.

Because the threat always rolls downhill, that is to say, adversaries always attack the weakest link. Information must be protected across the entire system. A three-sided castle is not very safe. Therefore, I contend that in almost all cases the cybersecurity requirements found in national security systems are identical to those found in e-commerce systems or critical infrastructures. It follows then that the research challenges, security features and development models are also quite similar.

With these similarities in mind, NSA has been working hard to converge these cybersecurity markets through a series of programs and research initiatives. Our goal is to leverage our deep understanding of cyber threat and vulnerability in a way that lets us harness the power and innovation provided by the information technology industry. We believe that the resulting cybersecurity solutions will protect all critical cyber systems, regardless of the information they process.

I think it will be useful for me to provide a brief description of NSA's cybersecurity responsibilities and authorities. I will then turn to the specific questions you asked me to answer in your invitation.

NSA Information Assurance Background

When I began working at NSA some 36 years ago, the "security" business we were in was called Communications Security, or COMSEC. It dealt almost exclusively with providing protection for classified information against disclosure to unauthorized parties when that information was being transmitted or broadcasted from point to point. We accomplished this by building the most secure "black boxes" that could be made, employing high-grade encryption to protect the information. In the late 1970s, a new discipline we called Computer Security, or COMPUSEC, developed. It was still focused on protecting information from unauthorized disclosure, but it brought with it some additional challenges and threats, e.g., the injection of malicious code, or the theft of large amounts of data on magnetic media.

With the rapid convergence of communications and computing technologies in the early 1980s and especially with the explosion of the personal computer, we soon realized that dealing separately with COMSEC on the one hand, and COMPUSEC on the other, was no longer feasible, and so the business we were in became a blend of the two, which we called Information Systems Security, or INFOSEC. The fundamental thrust of INFOSEC continued to be providing protection against unauthorized disclosure, or **confidentiality**, but it was no longer the exclusive point of interest.

The biggest change came about when these computer systems started to be interconnected into local and wide area networks, and eventually to Internet Protocol Networks, both classified and unclassified. We soon realized that in addition to confidentiality, we needed to provide protection against unauthorized modification of information, or data **integrity**. We also needed to protect against denial-of-service attacks and to ensure data **availability**. Positive identification, or authentication, of parties to an electronic transaction had been an important security feature since the

earliest days of COMSEC, but with the emergence of large computer networks, data and transaction **authenticity** became an even more important and challenging requirement.

Finally, in many types of network transactions it becomes very important that parties to a transaction cannot deny their participation, so that data or transaction **non-repudiation** joined the growing list of security services often needed on networks.

Because the term "security" had been so closely associated, for so long, with providing confidentiality to information, we adopted the term **Information Assurance**, or IA, within the Department of Defense to encompass the five security services of confidentiality, integrity, availability, authenticity and non-repudiation. I should emphasize here that not every IA application requires all five security services, although most IA applications for national security systems – and all applications involving classified information – continue to require high levels of confidentiality.

Another point worth noting is that there is an important dimension of Information Assurance that is operational in nature and often time-sensitive. Much of our work in IA is found in providing an appropriate mix of security services that are not operational or time-sensitive, e.g., education and training, threat and vulnerability analysis, research and development, assessments and evaluations, and tool development. However, in an age of constant probes and attacks of networks, an increasingly important element of protection deals with operational responsiveness in terms of **detecting** and **reacting** to these time-sensitive events. This defensive operational capability is closely allied with and synergistic with traditional IA activities, but in recognition of its operational nature is generally described as **Defensive Information Operations**, or DIO. NSA's responsibilities in this area have grown considerably since the late 1990's.

To meet this DIO challenge, NSA's National Security Incident Response Center (NSIRC) provides real-time reporting of cyber attack incidents, forensic cyber attack analysis, and threat reporting relevant to information systems. Through round-the-clock, seven-days-a-week operations, the NSIRC provides the Departments of Defense, the Intelligence Community, Federal Law Enforcement, Department of Homeland Security

and other Government organizations with information valuable in assessing current threats or defining recent cyber intrusions.

NSA's responsibilities and authorities in the area of information assurance are specified in, or derived from, a variety of Public Laws, Executive Orders, Presidential Directives, and Department of Defense Instructions and Directives. The Secretary of Defense is the Executive Agent for National Security Telecommunications and Information Systems Security. The Director of NSA has broad responsibilities in providing for the security of national security[1] telecommunications and information systems processing national security information, including:

- Evaluating systems vulnerabilities

- Acting as the focal point for cryptography and Information Systems Security

- Conducting Research and Development

- Reviewing and approving security standards and policies

- Conducting foreign liaison

- Assessing overall security posture

- Prescribing minimum security standards

- Contracting for information security products provided to other Departments and Agencies

- Coordinating with the National Institute of Standards and Technology (NIST); providing NIST with technical advice and assistance

---

[1] The Computer Security Act of 1987 defines national security systems as telecommunications and information systems operated by the US Government, its contractors, or agents, that contain classified information or, as set forth in 10 USC Section 2315, that involves intelligence activities, involves cryptologic activities related to national security, involves command and control of military forces, involves equipment that is an integral part of a weapon or weapon system, or involves equipment that is critical to the direct fulfillment of military or intelligence missions.

While protecting the confidentiality of classified information via extremely strong cryptographic systems was a major part of NSA's mission in the past, our mission has changed emphasis considerably over the last ten years. We now spend the bulk of our time and resources engaged in research, development and deployment of a full spectrum of IA technologies for systems processing all types of information. NSA's days of just building "crypto for classified" are long gone.

Specific Issues Related to Cybersecurity R&D

Your invitation outlined a number of areas where you wanted specific comments and answers.

1. Technical approaches to optimize cybersecurity.

I believe that the highest payoff for optimizing cybersecurity is the creation of an interoperable authentication system deployed widely throughout the federal, national security, first responder and critical infrastructure community. The typical approach used is a public-key-infrastructure (PKI) system with a smart card that contains your cyber credentials. This is the type of system that NSA and DISA have built for DoD. A national PKI system is required that allows for strong authentication in cyberspace for homeland security.

If we have this national system in the future—then when a first responder connects to a DHS website to access information or upload a report—we will know exactly who they are. We can then assign various privileges according to the role that the person is assuming for that specific information transaction. This authentication system also forms the basis for all of the other cybersecurity services from protecting the control of Supervisory Control and Data Acquisition (SCADA) systems to encrypting your email and passwords.

It is also important to note here that the most critical infrastructures, like a PKI, should be built using U.S. technology. I have concerns with foreign software of unknown trust and quality being integrated into critical U.S. systems.

My next priority for cybersecurity is effective border protection.   Just like our national borders or the perimeters of our buildings, we need to protect our cyber borders. Effective border protection includes many different technologies.

- The most important technology is a firewall. Firewalls help networks resist attacks by establishing a strong but resilient border between our protected network and the external Internet.

- We also need encrypted tunnels, also called virtual private networks or VPN's. These devices sit between critical networks to protect the information as it moves between secure networks over unprotected pipes.

- Another necessary border security technology is called a "guard". A guard is used when we need to share information between security domains. Consider the case of an intelligence report that is created on a top-secret network. It must be sanitized to unclassified and then sent to a local police department. It would be dangerous to allow this information to move between security domains without review. High assurance "guards" are designed to automatically and safely allow certain information packets to flow between systems but stops all others.

- Finally, effective borders require the ability to detect and respond to intrusions. Just like a security camera on a bank, cyber intrusion detection systems monitor the flow of information around your border and detect suspicious activity.

The best way to protect a system from attack is to eliminate its vulnerabilities. The best way to eliminate vulnerabilities is to improve the way we write software. High on my research priority list is the need for assured software design tools and development techniques. We also need to improve computer operating systems by including functionality to enhance their ability to defend themselves from attack.

The elimination of vulnerabilities is the goal but the reality is that we are a long way from achieving this goal. Attacks are common and vulnerabilities are discovered daily. It has been estimated that over 90% of all successful attacks on DoD systems are based on vulnerabilities that are already known and that have an updated software fix or "patch" available. The rare system operator can keep up with all of the "patches" that are issued each month. A system left un-patched soon becomes a target like an unlocked sports car with the keys in the ignition. Therefore, another way to optimize cybersecurity is with an automated patch management system.

This system would also use strong authentication as provided by a PKI but the software producer would sign the new application instead of a person. The patch would be automatically and safely sent to your system. The PKI guarantees that it is comes from an authentic source and has not been corrupted.

2. What areas of advanced technology should be pursued to outpace attacks?

Research is required to improve a cybersecurity system's ability to modify itself on-the-fly. New attacks are constantly emerging and new vulnerabilities are discovered even in the most carefully designed systems. The ability to update must be safely executed and as transparent to the user as possible.

NSA is working on a multi-year, nearly $3B development program called Cryptographic Modernization (CM) that has some of these features. There are over 1.3 million cryptographic devices in the U.S. inventory. Over 75% of these systems will be replaced during the next decade. Future security systems are being designed to use the network to safely program and reprogram their operating characteristics automatically and transparently to the user.

Research is also needed to learn how to build cybersecurity systems that can continue to operate even while under attack. Resilient systems, like those being investigated by DARPA and others will be needed in the future. The goal is to have a system that degrades gracefully instead of causing a cascade of insecurity.

I would also suggest that considerable research is needed to effectively coordinate information during a cyberattack. Today, most of this coordination occurs at the speed of humans. But attacks are carried out in seconds and are often carried out automatically.

The CODE RED attack in 2001 infected 50,000 machines per hour, ultimately causing billions of dollars in damage. We need a capability for our networks to work together automatically to weather an attack. Incident information formats, automatic remediation algorithms, the ability to learn attack specifics from intrusion detection devices and other network sensors and then share this info with other networks without human intervention are high priority requirements.

Another significant research topic is the ability to enhance attack identification methods. Most intrusion detection or system misuse systems today rely on patterns or signatures to identify the bad behavior. This works well for known attacks but is useless against novel attacks. The ability to detect attacks and misuse from anomalous behavior is needed.

The ability to detect suspicious or anomalous behavior is also useful to identify insider attacks. Studies have estimated that 50% of the most damaging attacks come from insiders. An insider is unlikely to use sophisticated attacks because they already have an account on the system–but the ability to monitor system use during off hours or track users accessing unusual accounts provides vital clues for detecting insiders.

Continuing with the cyber attack theme—I believe that one of the hardest problems we must solve in cybersecurity is attack attribution. That is the capability to geolocate and positively identify the source of attacks on the Internet. Without confident knowledge of who and where an attack was mounted, it is impossible to decide on the appropriate response. A rapid and reliable capability that separates nuisance hackers from more serious threats would increase the overall effectiveness of every cybersecurity practitioner in both government and the private sector. Effective attribution by law enforcement would also deter the casual hacker and allow resources to spent on more serious cases.

3. Suggest advanced technology programs needing higher priority & funding.

A significant cybersecurity improvement over the next decade will be found in enhancing our ability to find and eliminate malicious code in large software applications. Beyond the matter of simply eliminating coding errors, this capability must find malicious software routines that are designed to morph and burrow into critical applications in an attempt to hide. There is little coordinated effort today to develop tools and techniques to examine effectively and efficiently either source or executable software. I believe that this problem is significant enough to warrant a considerable effort coordinated by a truly National Software Assurance Center. This center should have representatives from academia, industry, federal government, national laboratories and the national security community all working together and sharing techniques to solve this growing threat.

We also need the ability to trust the hardware platforms we use for critical applications. Most microelectronics fabrication in the USA is rapidly moving offshore. NSA is working on a Trusted Microelectronics Capability to ensure that state-of-the-art hardware devices will always be available for our most critical systems.

The DoD is currently undertaking a major program called transformational communications. This program is developing the military communications infrastructure of the future and it will be delivering high-bandwidth, secure, multi-faceted digital capabilities across the defense enterprise and down to the individual warfighter. Many new cybersecurity requirements are being generated by this initiative and they will require significant R&D resources. For example, additional key management infrastructure capabilities, techniques for multi-level security networks, and ultra-high bandwidth encryption are a few of the new technologies being driven by this requirement. It is important to note that the results of this program will be dual-use. The technology being developed will have application for solving many of the same challenges that are found in homeland security systems.

In today's Information Technology environment, the need is particularly acute for ways to counter security vulnerabilities found in popular commercial operating systems

and applications. While many of these vulnerabilities can be fixed by properly configuring the system, the goal is to configure these systems to be as secure as possible "right out of box." Building on the hugely popular security configuration guides for Windows 2000, NSA, working with Defense Information Systems Agency, the National Institute of Standards and Technology, the FBI's National Infrastructure Protection Center (now at DHS), the General Services Administration's FedCert, the SANS Institute, the Center for Internet Security and vendors—developed a set of consensus benchmark security standards. These standards provide a sort of "preflight checklist" of security settings.

The benchmark standards represent an effective model based on agreement between security experts, system operators and software vendors. A number of standards for the most popular technologies are being adopted by many government and private sector CIOs.

I am happy to learn from your last hearing that some equipment vendors are now offering the security standards as the default configuration. I also understand from your hearing last week that industry gave high marks to the great work being done by the Center for Internet Security. NSA is proud to be a part of this project and will continue to support the community in establishing security standards. This consensus approach may not eliminate every vulnerability, but by working together, we can harden our systems against common attacks.

4. Role of technology transfer among government, academia, and industry?

NSA is motivated by a sincere belief that the requirements for cybersecurity products and services for national security uses are identical to the requirements found in other mission critical systems e.g., homeland security and critical infrastructure protection. We have developed a number of programs and policies targeted leveraging the commercial information technology.

- The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation,

and assessment needs of both information technology producers and consumers. NIAP is collaboration between the National Institute of Standards and Technology and the NSA in fulfilling their respective responsibilities under the Computer Security Act of 1987. The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. The long-term goal of NIAP is to increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the nation's critical information infrastructure.

- NIAP also produces cybersecurity specifications, called protection profiles that have already been developed for low and medium assurance applications and are periodically updated. The profiles are available on the NIAP website for anyone to use to describe the features needed for cybersecurity applications.

- NSTISSP #11 (National Security Telecommunications and Information Systems Security Policy #11) is a national security community policy governing the acquisition of information assurance products. The policy mandates, effective 1 July 2002, that departments and agencies within the Executive Branch shall acquire, for use on national security systems, only those products that have been validated in accordance with the either the Common Criteria, or other approved methods. Additionally, NSTISSP # 11 notes that departments and agencies may wish to consider the acquisition of validated COTS products for use in information systems that may be associated with the operation of critical infrastructures as

defined in the Presidential Decision Directive on Critical Infrastructure Protection Number 63.

- The Information Assurance Technical Framework Forum (IATFF) is a NSA sponsored outreach activity created to foster dialog between U.S. government agencies, industry, and academia seeking to provide their customers solutions for information assurance problems. The ultimate objective of the IATFF is to agree on a framework for information assurance solutions that meet customers' needs and foster the development and use of solutions that are compatible with the framework. The forum serves to increase awareness of available security solutions and allows attendees to establish contacts with other individuals and organizations dealing with similar problems. The Information Assurance Technical Framework document, currently in its third revision that provides over 500 pages of technical guidance for protecting information and information systems.

- The Centers of Academic Excellence in Information Assurance Education Program is an outreach effort designed and operated by NSA in the spirit of Presidential Decision Directive 63. The program goal is to reduce vulnerability in our National Information Infrastructure by promoting higher education in information assurance, and producing a growing number of professionals with IA expertise in various disciplines. Fifty universities have been designated as Centers of Academic Excellence to date. NSA has also been using the skills found at the service academies in a number of interesting ways. One exciting program is the service academies competition for attacking and defending networks. We also sponsor visiting professors in IA. We need this type of program for our workforce development - we must invest in our future.

- NSA is also working to transfer techniques to cybersecurity service providers. One of the services that NSA offers under this authority is

system security assessment. Since NSA has limited resources to meet the ever-growing demand for INFOSEC Assessments, a training and certification program was developed as a partnership between NSA and private INFOSEC Assessment providers.

- NSA also created the INFOSEC OUTREACH Program to combine the substantial Information Systems Security talents of government and industry partners. The program provides insight into secure design, security evaluation, and the security considerations of system certification. Working together, the partnership of government and industry can meet the increasing demands for state-of-the-art secure telecommunications and information systems.

- NSA and the International Information Systems Security Consortium (ISC)2 developed a new Information Systems Security Engineering Professional credential for information security professionals who want to work on national security systems. The new certification will serve as an extension of the Certified Information Systems Security Professional, offered by (ISC)2 for information security.

5. How are research priorities and programs determined in the national security area?

We base our priority decisions on a number of factors. The first factor is determined by the technologies and systems most used by our customers. For example, we recently started a comprehensive R&D program to enhance the security of PDA's and wireless 802.11 networks over the last two years because of the explosion of the use of these systems by our DoD customers.

We also maintain a large number of cooperative research agreements with many of the most important technology vendors to help us keep ahead of their development cycles. We also work with small firms ensuring that their innovative technologies are fully informed by our cybersecurity expertise. This insight allows us to program for

anticipated cybersecurity enhancements of our systems, or in the best case, influence our industrial partners, large and small, to add additional IA features during development.

Our researchers also participate in R&D agenda setting panels and boards with the NSF, DARPA, National Laboratories, and industry associations. We collaborate with the R&D functions in our customer's organizations. All of this information is used in making an R&D priority and programming decision.

NSA is also unique in that we have considerable insight into the threat presented by various adversaries from our intelligence activities. Threat profiles are developed and these, in part, drive our research agendas.

6. Share your perspectives on leveraging national security standards for homeland security needs?

National security standards are developed for—and are intended to be leveraged for all critical cybersecurity requirements.

- In order to promote secure interoperability between wired and wireless systems NSA initiated an industry and government consortium to agree on a common signaling plan called the future narrowband digital terminal (FNBDT). Although in reality it is not just narrow band anymore but a broad specification, FNBDT includes a common voice processing capability, a common signaling protocol, a common crypto-algorithm base, and a common key management process. FNBDT has become the primary security standard for cell phones, military radios and many emerging public safety communications devices intended to serve homeland security missions and first responders all around the world.

- We also created the High Assurance IP Interoperability Specification (HAIPIS), which will ensure interoperability with all future generations of IP network encryptors.   The IP, or Internet protocol, is the backbone of the worldwide Internet. This new cybersecurity specification has become

extremely popular and new products, based on this specification are being released regularly.

- Many of the technologies that we are suggesting for homeland security requirements were developed to support coalition military warfare. These systems were designed to cost-effectively support a highly mobile and constantly changing set of information sharing partners. We are confident that they are exactly what many homeland security applications require.

Conclusion

It has been my pleasure to share the work of my agency with the committee today. I believe that much of the research and development initiated by NSA for use in the national security community is directly transferable to the needs of homeland security. We all need to work together to shape the demand side of the market. Everyone needs trustworthy technology. We cannot afford to cut corners.

We must change our fundamental assumption from need-to-know to need-to-share. We must share policies and processes across the community. Cybersecurity products and technologies have been the focus of my remarks today but the technology alone will never be good enough to protect us because— ultimately—getting cybersecurity right is more about what you do than what you buy.

Thank you for the opportunity to speak before the subcommittee today.