National Security Agency

Statement by

Mr. Daniel G. Wolf

Information Assurance Director

National Security Agency

Before the

House Committee On Government Reform

Subcommittee on

Government Efficiency, Financial Management and Intergovernmental Relations

and the

Subcommittee for

Technology and Procurement Policy

Joint Hearing on

H.R. 3844: The Federal Information Security Reform Act of 2002

2 May 2002

Good morning Chairman Horn, Chairman Davis, and distinguished members of both Subcommittees. I appreciate the opportunity to be here today to talk about information technology security as your subcommittee considers H.R. 3844 "The Federal Information Security Reform Act of 2002". While I am not in a position to express the Administration's views on H.R. 3844, I thought it might be helpful if I shared our technical experience with you.

I also would like to thank the Members of both Subcommittees for their consistently strong interest and attention to this vital area over the past few years. Your leadership is providing a genuine public service in raising the visibility of the serious security challenges we all face in an age of interconnected, inter-dependent digital 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. While some may suggest that NSA's perspective is too narrow due to our focus on the stringent requirements of national security systems, I would like to note that NSA's Information Assurance Directorate and its predecessor organizations have had policymaking and implementation responsibility regarding the protection of national security telecommunications and information processing systems across the Executive Branch since 1953.

During our nearly 50 years of producing not only security policies but also in the hard work of deploying security products and services that implement those policies, we have learned—and in this we agree with many members of this committee—that successful information security demands aggressive management oversight, extensive sharing of best practices, and a bedrock foundation of proven security standards. There are a number of areas of the bill in which, from the perspective of information security technology, improvements are needed, such as:

1. Defining and identifying national security and mission critical systems

2. Risk assessment and system interconnection management

3. Conducting annual evaluations

4. Coordinating policies

5. Coordinating incident detection and consequences management

6. Sharing vulnerability information

I believe it is useful to provide a brief description of the responsibilities and scope of NSA in the area of Information Assurance (IA) and NSA's policymaking functions and authorities.

NSA Information Assurance Background

When I began working at NSA some 33 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 equipment to protect information. In the late 1970s, and especially in the early 1980s with the advent of the personal computer, a new discipline we called Computer Security, or COMPUSEC, developed. It was still focused on protecting information from unauthorized disclosure, but 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, 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 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 became very important that parties to a transaction not 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, within the Department of Defense we adopted the terms **Information Assurance**, or IA, 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 the work of Information Assurance in providing an appropriate mix of security services is not operational or time-sensitive, i.e., education and training, threat and vulnerability analysis, research and development, assessments and evaluations, and tool development and deployment. In an age of constant probes and attacks of on-line networks, however, 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 and synergistic with traditional Information Assurance activities, but in recognition of its operational nature is generally described as **Defensive Information Operations**, or DIO.

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 (NSTISS). The Director of NSA is the "National Manager" for NSTISS. The Director of NSA has broad responsibilities for the security of national security telecommunications and information systems, including:

- Evaluating systems vulnerabilities
- Acting as the focal point for cryptography and Information Systems Security
- Conducting research and development in this area
- Reviewing and approving standards
- Conducting foreign liaison
- Operating printing and fabrication facilities
- Assessing overall security posture
- Prescribing minimum standards for cryptographic materials
- 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

The incumbent Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD/C3I), currently Mr. John Stenbit, chairs Committee on National Security Systems (CNSS), which is a committee of the President's Critical Infrastructure Protection Board under Executive Order 13231, Critical Infrastructure Protection in the Information Age, on October 16, 2001.

The Committee performs a number of important functions, including advising on the release of information systems security equipment and information to foreign governments and organizations – usually for military interoperability purposes – through a careful assessment and voting process. The Committee's primary function primary function is to coordinate and advise on Information Assurance policies.

NSA has several key roles in the CNSS. As noted above, the Director of NSA is the "National Manager" for National Security Telecommunications and Information Systems Security, and as such signs the CNSS' issuances. NSA also provides day-to-day support to and management of CNSS activities by providing a senior official to act as the organization's Executive Secretary. Most importantly, NSA provides a permanent Secretariat of full-time staff personnel, facilities, and other necessary support such as funding, printing and distributing documents, sponsoring a Web site, managing voting processes, maintaining official records, developing policy and doctrine proposals, and organizing committee, subcommittee, and working group meetings, as well as an annual conference.

Specific Comments to H.R. 3844

1. Defining and identifying national security and mission critical systems

We suggest that the modified definition found in the amended Section 3532 may possibly add confusion to the already complex process of identifying 'national security systems' by adding another source rather than citing an existing source for defining the term as was done in the original GISRA language. We also believe that that there are significant parallels found in identifying, characterizing and protecting mission critical systems and national security systems as we learned by our collective efforts to determine critical dependencies between computer systems during the Y2K crisis. Therefore we suggest returning to the language as specified in the original GISRA Section 3532 (b)(2).

In a related matter, the provision that directs NIST to develop 'guidelines for identifying an information system as a national security system' in the amended Section 20 (b)(3) of the National Institutes of Standards and Technology Act (15 U.S.C. 278g-3)

is unnecessary inasmuch as national security systems are defined in existing law, specifically the Clinger-Cohen Act of 1996 and the Government Information Security Reform Act.

2. Risk assessments and system interconnection management processes

There are a number of references throughout H.R. 3844 where the concepts of risk assessment and risk management are included. It has been our experience that comprehensive and useful risk assessments are extremely difficult to initially complete and even harder to maintain throughout a system's lifetime. This problem gets potentially dangerous when you consider that systems that are independently assessed for risk are soon interconnected. One organization's calculation for acceptable risk may be very different from another's. But in the richly interconnected world of federal systems—a risk taken by one system is ultimately borne by all the others.

We suggest that the committee consider assigning a high priority to the development of a comprehensive standard for federal system risk assessment and management. The standard should describe—not only the assessment process and documentation requirements—but also include standard methods for characterizing adversarial threats and capabilities, determining categories for mission impact and offer a method for ensuring that the assumptions used in the risk assessment are adjusted as appropriate over time.

A risk assessment—in an interconnected world—cannot be simply completed at the time a system is certified and then filed away. It must become a living document, a sort of trusted calling card that is used when two systems are negotiating their interconnection. The quality of the risk assumptions, calculations and decision thresholds cannot be safely left to chance or independent decisions. There must also be a common method throughout the federal government for managing system interconnection based on a standardized approach to risk assessment. Otherwise, the weakest link in the chain will most certainly break.

3. Conducting annual evaluations

We suggest that Section 3535(b) as amended by HR 3844, mandating that annual evaluations for each agency with an Inspector General be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General be reconsidered. It is our experience that the necessary technical competence to either conduct the evaluation or to specify the terms for an information system security effectiveness assessment may not always reside with the Inspector General. We recommend that subsection (b) be deleted, and that it be replaced by subsection (c), amended to provide that in all cases the department or agency head shall determine what internal or external body will perform an annual evaluation.

4. Coordinating policies

Section 3533(a)(3) encourages the coordinated development of standards and guidelines with agencies and offices operating national security systems. We suggest that additional efficiencies could be gained by requiring the Director in cooperation with the CNSS, to annually conduct a complete review of all related 'national security systems' policies, practices, guidelines, and standards to identify and report on those that are most relevant and prioritize a complementary publication schedule.

5. Coordinating incident detection and consequences management

The Federal information security incident center described in Section 3536 has confused us. We offer no comment if this section is intended to provide authorizing language for the existing Federal Computer Incident Response Center (FedCIRC) operated by the General Services Administration. However, if this section were intended to propose an additional federal incident management center then we would respectfully ask the committee to reconsider.

The defense of both the National Information Infrastructure (NII) and the Defense Information Infrastructure (DII) require a robust and time-sensitive Defense-in-Depth approach. To help meet this challenge, NSA's National Security Incident Response Center (NSIRC) provides near 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 and other Government organizations with information valuable in assessing current threats or defining recent cyber intrusions.

The NSIRC at NSA has established a trusted relationship and a proven set of analytical and reporting processes with the FedCIRC. Moreover, we have similar relationships with the National Infrastructure Protection Center (NIPC) and the Department of Defense's Incident Center (DODCERT) that were created over the past 3 years.

We believe that adding a new federal incident management center would add unnecessary redundancy and decrease both the efficiency and effectiveness of the community and the NSIRC.

6. Sharing vulnerability information

We agree that it is extremely important for all federal agencies and departments to develop effective procedures for the timely dissemination of information system security vulnerability information. However, we also believe that this information must be controlled and disseminated with the utmost care and only after thorough consideration regarding the possible consequences not just to an organization's local systems—but to all related federal systems.

Today's information technology is a veritable monoculture. There is very little diversity in the underlying technology and therefore the security vulnerabilities found in national security systems as compared with other federal systems. Section 3535(c)(2) of the proposed amendment requires appropriate protection of information security vulnerability information. However, we would encourage the committee to consider adding language that provides for the appropriate protection of this type of information regardless of the system from which it was derived.

This concludes my testimony and Statement for the Record. I will be pleased to answer any questions you may have.