STATEMENT SUBMITTED

BY THE

UNITED STATES NUCLEAR REGULATORY COMMISSION

TO THE

HOUSE GOVERNMENT REFORM COMMITTEE

SUBCOMMITTEE ON

TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS

AND THE CENSUS

UNITED STATES HOUSE OF REPRESENTATIVES

CONCERNING

"INFORMATION SECURITY IN THE FEDERAL GOVERNMENT: ONE YEAR INTO THE

FEDERAL INFORMATION SECURITY MANAGEMENT ACT"

SUBMITTED BY

MR. ELLIS W. MERSCHOFF

CHIEF INFORMATION OFFICER

SUBMITTED: MARCH 16, 2004

Mr. Chairman and Members of the Subcommittee, I want to thank you for this opportunity to testify with regard to the activities of the U.S. Nuclear Regulatory Commission (NRC), as they relate to the Federal Information Security Management Act (FISMA).

I will outline the NRC's responsibilities and the security issues that arise in meeting those responsibilities. I will then address the NRC's efforts to achieve FISMA compliance, and will highlight a few of the NRC's information technology (IT) systems.

The NRC was created as an independent regulatory agency in 1975, taking over the regulatory functions of the former Atomic Energy Commission. The mission of the NRC is to regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment. The NRC's scope of responsibility includes regulation of commercial power plants; research, test, training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and waste.

Our headquarters is located in Rockville, Maryland, with regional offices located in Pennsylvania, Georgia, Illinois, and Texas. We also have a technical training center located in Tennessee, and we have resident inspector sites located at 70 nuclear plant and fuel cycle facilities around the country. For Fiscal Year 2004, the agency has a budget of $626 million and staffing of 3,059 full-time equivalents (FTE).

The NRC is headed by five Commissioners, who are appointed by the President and confirmed by the Senate to serve for five-year terms. The Executive Director for Operations (EDO), currently Dr. William D. Travers, carries out the policies and decisions of the Commission and oversees the agency's day-to-day operations. The Office of the Chief Information Officer (OCIO) is one of 15 headquarters and regional offices under the direct purview of the EDO.

The NRC recognizes the importance of providing a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets and provides for development and maintenance of controls required to protect Federal information and information systems. The NRC has historically been focused on technical safety and security issues, and computer security is another facet of that overall concern. Congressional oversight and participation in Federal CIO groups have helped focus our computer security efforts to more effectively protect our computer systems. NRC has had a computer security program since 1980 and has adequately budgeted for the agency's information technology requirements. Our focus on computer security from project inception and throughout the project life cycle has enabled us to appropriately protect our computer systems.

As an agency, we have 4,000 interconnected computers that exchange approximately 100,000 email messages and receive another 40,000 email messages from the Internet every day. On a daily basis, we intercept an estimated 2,500 SPAM messages; experience 500 attempts at reconnaissance of our systems; strip out 300 suspicious email attachments; identify

100 attempts at denial-of-service attacks; and isolate 10 virus occurrences. In 2003, our monthly status reports to the Federal Computer Incident Response Center (FedCIRC) recounted more than 67,000 non-debilitating incidents.

The agency's external Web site comprises approximately 30,000 pages of information, which are visited an average of 350,000 times per month, by people in 175 countries, for a total of more than 3,000,000 pages viewed each month. Each year, we publish approximately 200 nuclear regulatory documents, edit about 15,000 pages, and respond to thousands of requests for information in the library and public document room.

As I mentioned, the NRC has had a formal computer security program in place since 1980. As the basis for that program, the NRC follows Federal guidance from the Office of Management and Budget (OMB), the National Security Agency (NSA), the General Accounting Office (GAO), and the National Institute of Standards and Technology (NIST). We also participate in a variety of related Federal organizations, including the Computer Security Program Managers' Forum, the Federal Information Systems Security Educators' Association, and the Committee on National Security Systems and its working groups. In addition, we interact with the Department of Homeland Security (DHS), FedCIRC, the Computer Emergency Response Team at Carnegie Mellon, the Computer Incident Advisory Capability under the Department of Energy, and other recognized computer security organizations with which we cooperatively monitor situations and share alerts, methods of dealing with problems, and related information.

The NRC considers the agency's overall computer security needs alongside other funding requests, and the computer security needs of projects are an integral part of our capital planning and investment control process. We carefully review IT-related budget submissions to ensure that computer security is appropriately included. OMB approved the NRC's major IT system Capital Asset Plans and Business Cases Exhibit 300s with overall high ratings of "4" and "5," with "5" being the best possible rating. This approval of every NRC Exhibit 300 verifies that the agency employs sound project management, presents a strong business case for each IT investment, and meets other administration priorities to define the cost, schedule, and performance goals for each investment. Scoring criteria include support for the President's Management Agenda, acquisition management, performance goals, security and privacy, performance-based management, and life-cycle costs.

The NRC's management directives define agency policy and are the foundation upon which all agency work is performed. The "Automated Information Systems Security Program Management Directive" defines the NRC's computer security policy and defines applicable organizational responsibilities and delegations of authority. This document also includes a handbook, which the agency uses to implement the policy, referring to other Federal guidance as appropriate.

The NRC has identified all major operational applications and general support systems, each of which has been certified and accredited. Outstanding findings from risk assessments, system security plans, security tests and evaluations, contingency plan tests, certifications, and accreditations are entered into a tracking system, monitored, and closed out when resolved.

We also review the security controls for each of these systems on an annual basis, using the self-assessment process provided by NIST. Each system must be recertified and accredited every three years or when a major modification is made to the system. New system developments or system modifications are reviewed for computer security issues at appropriate steps of the system development life cycle.

Another contributing factor to the success of the NRC computer security program is the strong working relationship between my staff and the staff of the Office of the Inspector General. Identified security issues are raised as they are found and discussed throughout the year in a collegial environment between the two offices to aid in issue resolution.

The NRC emphasizes computer security awareness at all levels of the organization, from senior management all the way down to the individual employee and contractor. The NRC requires that each employee take an annual computer security awareness course. The NRC has implemented this course as an online resource, to ensure accessibility at the employee's desktop. The online course presents topic area information, followed by a short quiz that enables the employee to determine how well he or she understood the information. Each employee can raise questions about the course and its content, make suggestions for improvement, request test modification throughout the course, and return to the course whenever he or she wishes to review particular segments. By the end of 2003, 98.5 percent of our employees, interns, and contractors had satisfactorily completed the course. We track completion by office and report to each office how many of the staff members have completed the course and how this number relates to the completion rate of other offices. This friendly competition has helped to improve participation.

The NRC also has an online course for Information Systems Security Officers (ISSOs), which 100 percent of our ISSOs have completed. While only 33 agency employees have significant IT security responsibilities and are required to take this course, an additional 255 employees and contractors have taken the ISSO course to further their knowledge and understanding of information security.

The OCIO also hosts an annual observance of International Computer Security Awareness Day, which has grown in participation over the past 10 years. In November 2003, close to half of our headquarters population attended this event. In hosting this annual event, we use different themes each year. The day begins with a special guest speaker, followed by vendor exhibits in our exhibit hall. Our computer security staff representatives distribute informative brochures, as well as anti-virus software for employees to use on their home machines (as permitted by our site license.) We also have a year-round rotating poster campaign in all elevator lobbies of the headquarters and regional facilities.

Like all Federal agencies, the NRC must contend with viruses and other malicious software, and we expeditiously deal with the presence of such software within the NRC's network through isolation and extermination. We automatically download virus definitions to all desktops to ensure the currency of the information, and we deploy relevant computer security patches as soon as testing ensures compatibility with the NRC's mission-related software. The NRC also utilizes Network Announcements (distributed via email and on our internal Web site) to notify staff about viruses, hoaxes, SPAM, and scams that might affect our staff while at work or even on their personal computers at home. Our computer security staff representatives also contribute articles to the NRC's monthly "News, Reviews, & Comments" newsletter. "Ask

CyberTyger" is a regular column in the newsletter that seeks to answer employees' computer security questions. Our computer security staff created CyberTyger about eight years ago to act as a spokesman and logo character to convey our computer security messages. This character has since been replicated and used by other Federal agencies.

It is also appropriate to note that the NRC is the only Federal agency with a comprehensive electronic document management system, known as the Agencywide Documents Access and Management System (ADAMS), for which the agency received the Archivist of the United States Award of Excellence. ADAMS supports the creation or capture, storage, retrieval, management, and dissemination of documents and records related to the NRC's core business functions, such as the licensing and regulatory oversight of nuclear reactor operations and other activities involving regulation of nuclear materials and nuclear waste. Access to these documents by both NRC staff and the public is essential to enable the NRC to carry out its mission. The system captures documents upon receipt or signature, and stores them electronically in a single central location or repository, rather than in numerous office-level locations, thereby ensuring the integrity and availability of the document collection. The system also allows for electronic distribution of incoming documents, thereby eliminating substantial paper duplication efforts and making documents more quickly available for review. Because ADAMS makes documents available in electronic form, the system improves efficiency by effectively facilitating the re-use of documents by agency staff. The system also stores the agency's record copy in electronic form for efficient transfer to the National Archives and Records Administration. In addition, users can search for, view the image of, and print documents at their workstations, regardless of geographic location. As a result, documents are

now available to the public in minutes rather than weeks, and can be viewed and downloaded at no charge.

ADAMS customers and stakeholders include all NRC staff and licensees; law firms; various public interest groups and professional organizations; medical offices and hospitals; schools, universities, and students; many local, State, and Federal government agencies; and other members of the public. Nonetheless, access to documents stored in ADAMS is contingent upon the nature of the document. Some documents are available to everyone, but others can be viewed only by those with the proper authorization. ADAMS software identifies and authenticates users and applies access controls to ensure that each document is viewed or modified only by appropriate individuals.

The NRC receives electronic copies of documents from agency stakeholders, including the public, through our Electronic Information Exchange (EIE) system. EIE provides the capability to securely receive material related to official agency business from NRC customers and other Federal agencies across the Internet. The EIE system uses public key infrastructure and digital signature technology to authenticate documents, validate the identity of the person submitting the information, encrypt submitted data for storage in the EIE database, and decrypt stored data during retrieval from the database. This supports voluntary electronic submission of documents by interested parties to official agency proceedings, including licensees under Title 10, Part 50, of the *Code of Federal Regulations* (10 CFR Part 50).

Coupled with EIE, the NRC's Licensing Support Network (LSN) portal is the mechanism by which the parties (and potential parties) to the future high-level waste repository licensing

adjudication are to make all relevant documentary material available. The LSN replaces the classic "discovery" document exchanges among parties with electronic access to discovery materials beginning prior to the docketing of a license application. The Web-based LSN portal (www.lsnnet.gov) connects each party's document collections on whatever hardware and software platform they choose, within general guidelines reflecting agreed upon standards and formats.

In summary, the NRC operates with offices across the Nation and interacts with the public in general informational, regulatory, and discovery interchanges. In each of these interchanges, we take the inherent computer security requirements very seriously and work toward a seamless integration of computer security in our day-to-day operations. The NRC's computer security challenges continue to evolve, and we continue to revise our computer security program to address these new requirements.

I appreciate the opportunity to appear before you today and I would be pleased to answer any questions you may have.

# # #