STATEMENT OF DARREN B. ASH
DEPUTY EXECUTIVE DIRECTOR FOR INFORMATION SERVICES AND CHIEF INFORMATION OFFICER
U.S. NUCLEAR REGULATORY COMMISSION

BEFORE THE

SUBCOMMITTEE ON FEDERAL FINANCIAL MANAGEMENT, GOVERNMENT INFORMATION, FEDERAL SERVICES, AND INTERNATIONAL SECURITY
COMMITTEE ON HOMELAND SECURITYAND GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

March 12, 2008

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to appear today to discuss the U.S. Nuclear Regulatory Commission's (NRC's) efforts to protect its information technology assets and sensitive information.

As the Deputy Executive Director for Information Services and the agency's Chief Information Officer (CIO), I report directly to the Executive Director for Operations and oversee information management and information technology activities agency-wide.

To provide some context for today's hearing, I would like to outline the NRC's mission and the information-related security challenges that arise in meeting those responsibilities.

Background on NRC and IT Security Challenges

The mission of the NRC is to license and regulate the Nation's civilian use of byproduct, source, and special nuclear materials to ensure adequate protection of public health and safety, promote the common defense and security, and protect the environment. The NRC's scope of responsibility includes the regulation of commercial nuclear power plants; research, test, and training reactors; fuel cycle facilities; medical, academic, and industrial uses of nuclear materials; and the transport, storage, and disposal of nuclear materials and waste.

The NRC headquarters complex is located in Rockville, Maryland, and we maintain regional offices located in Pennsylvania, Georgia, Illinois, and Texas. The NRC also has resident inspectors assigned at all nuclear power plants and the most significant fuel cycle facilities around the country. We also have a technical training center located in Chattanooga, Tennessee.

The NRC has over 4,300 interconnected computers that exchange approximately 183,000 email messages daily. The agency's external Web site comprises over 35,000 pages of information, which are visited by people in over 200 countries, for a total of about 3.7 million pages viewed each month. In addition, in 2007, the NRC released over 66,000 new documents for public access through our centralized document and records management system that is accessible through NRC's public Web site.

The NRC is very much aware of the magnitude of the computer security challenge and the importance of strengthening defenses to meet it. Along with other agencies, the NRC has experienced an escalation of attacks from hackers and others who wish to damage the Federal IT infrastructure. Attempts to penetrate agency networks continue to increase, computer viruses proliferate, and unscrupulous individuals are devising more clever ways to entice users, including Federal employees, to open damaging attachments or provide information to spurious Web sites.

On a monthly basis, the NRC blocks an estimated 4.7 million malicious emails. The NRC blocks the malicious emails using reputation filtering; and blocks email sent from sites/domain with a bad or malicious reputation. The NRC further filters 800,000 emails, which typically include over 31,000 "potential" SPAM messages, over 50 e-mail viruses, and over 900 suspicious e-mail attachments. On a daily basis, the NRC experiences over 500 attempts at reconnaissance of its systems, over 390 attempts to exploit the web server(s), at least 5 attempts at denial-of-service attacks, and typically 2 virus occurrences. In 2007, our monthly status reports to the U.S. Computer Emergency Response Team (US-CERT) identified more than 333,000 non-debilitating incidents.

Despite these numbers, the NRC has had to report relatively few intrusions to law enforcement. Specific denial of service attempts were lower for 2007, in part, due to discrepancies in how different intrusion detection system vendors classify denial of service attacks and improvements in the attack analysis, eliminating a large number of false positives. Further, the US-CERT Concept of Operations (ConOps) specifies limited conditions for reporting incidents to law enforcement.

NRC's IT Security Program

The NRC recognizes the importance of providing an effective IT Security Program that is compliant with the Federal Information Security Management Act (FISMA), as well as with the Office of Management and Budget (OMB), and National Institute of Standards and Technology (NIST) guidance. This program must ensure the effectiveness of security controls over information resources and assets. While a computer security program has been in existence at the NRC since 1980, the agency established a new organization, the Computer Security Office (CSO), as the focal point for agency-wide efforts. In addition to addressing the core requirements of FISMA, the CSO works with other NRC offices on strategies to protect sensitive information.

Protection of Sensitive Unclassified Information

In addition to protecting classified information, the NRC generally stores and processes two types of sensitive unclassified information in the course of fulfilling its safety and security mission.

The first category is termed Safeguards Information (SGI). SGI is a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act of 1954, as amended, pertaining to the measures used to safeguard nuclear facilities and materials. While SGI is sensitive unclassified information, it is handled and protected similar to classified confidential national security information, unlike other sensitive unclassified information (e.g., privacy and proprietary information). Access to SGI requires a favorable Federal Bureau of Investigation (FBI) fingerprint check, an indication of trustworthiness normally obtained through a background check, and a valid need-to-know.

The unauthorized release of SGI could result in harm to public health and safety and the common defense and security. Release could also result in the potential to impact the country's nuclear power plants and other facilities and materials licensed and regulated by the NRC.

Information designated as SGI must be protected from unauthorized disclosure and is physically controlled and protected. Protection requirements include secure storage, restricted access, document marking, limited reproduction, protected transmission, controls for information processing on electronic systems, and controls for destruction. SGI information is physically and logically stored, and processed separately from the rest of the agency's information technology.

The second category is Sensitive Unclassified Non-Safeguards Information (SUNSI). SUNSI is defined as any information of which the loss, misuse, modification, or unauthorized access can reasonably be foreseen to harm the public interest, the commercial or financial interests of the entity or individual to whom the information pertains, the conduct of NRC and federal programs, or the personal privacy of individuals. The groups of SUNSI include Privacy Act and Personally Identifiable Information (PII); allegation information; investigation information; proprietary information; Federal, State, foreign government, and International Agency-Controlled Information; security-related information; and sensitive internal information.

The NRC considers the protection of SUNSI, including personally identifiable information a serious matter. While SUNSI "spills" have occurred and may occur again, I believe that the policies, processes, procedures and protections in place are strong.

Over the last couple of years, the OMB and NIST have defined concrete actions agencies must take to protect unclassified sensitive information better. As reported by the Government Accountability Office (GAO) in their January 2008 report, "Information Security: Protecting Personally Identifiable Information," the NRC has addressed some, but not all of the critical actions. Specific accomplishments and actions of note include:

- Designating the Deputy Chief Information Officer as the Senior Agency Official for Privacy, as required by M-05-08, "Designation of Senior Agency Official for Privacy".
- Conducting a review of NRC's policies and processes, to ensure NRC has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to PII, as required in M-06-15, "Safeguarding Personally Identifiable Information." The results of the review were provided in the FY 2006 annual FISMA report.
- Issuing on June 22, 2006, an agency-wide announcement entitled "Safeguarding Personal Privacy Information" reminding all NRC employees and contractors of their responsibilities to safeguard PII from unauthorized access.
- Providing, along with NRC's FY 2006 annual FISMA report, the results of the Senior Agency Official for Privacy's review per OMB memorandum M-06-15, an Office of Inspector General (OIG) list of systems missing from NRC's inventory of major systems.
- Issuing on September 19, 2006, a policy entitled "Protection of Personally Identifiable Information," to implement provisions of M-06-16, "Protection of Sensitive Agency Information," that:

  - Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted[1], unless a waiver is granted;
  - Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices;
  - Prohibits staff from using personally-owned computers for processing or storing PII pertaining to NRC official business other than their own PII;
  - Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted;
  - Restricts remote access to PII information on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout;
  - Prohibits emailing of PII outside of NRC's infrastructure except where necessary to conduct agency business; and
  - Requires the logging and a retention assessment of PII extracts.

- Issuing on September 19, 2007, the "U.S. Nuclear Regulatory Commission Personally Identifiable Information Breach Notification Policy" and the "U.S. Nuclear Regulatory Commission Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers," as required by M-07-16, "Safeguarding Against and Responding to the Breach of PII." NRC staff was notified of both the breach notification policy and the plan to eliminate the unnecessary collection and use of Social Security numbers via an agency-wide announcement on September 19, 2007. As required by the memorandum, these documents are publicly available on the NRC's Web site at: http://www.nrc.gov/site-help/privacy.html#ssn.

Two recent examples that represent specific actions to protect NRC information systems and sensitive information are NRC's implementation of the Federal Desktop Core Configuration and the development of the National Source Tracking System:

Federal Desktop Core Configuration Compliance

NRC is working towards compliance with the Federal Desktop Core Configuration (FDCC) initiative. The FDCC is a set of information security controls or settings to be implemented on all Federal desktops running Microsoft XP or Vista. By implementing FDCC, the NRC will have a stronger baseline level of security, reducing risks from IT security threats and vulnerabilities. Even prior to February 2008, the NRC met or exceeded 213 of 237 NIST suggested settings (90 percent). The NRC will implement an additional 14 settings by May 2008, totaling 96 percent of the suggested settings. With regard to Application/Registry Settings, the NRC meets or exceeds 37 of 62 NIST suggested settings (60 percent). The NRC will implement an additional 12 settings by May 2008, totaling 79 percent of the suggested settings. The NRC will determine the path forward to close the gap in both instances, especially as the gap impacts user operations.

[1] The NRC does not currently have the resources to encrypt data on all mobile computers or devices. The NRC plans to take additional action to address this issue, along with the other technical requirements established by M-06-16.

National Source Tracking System

Radiation sources are used in many medical, industrial and research applications that are critical to the nation's health, safety and economic strength. To improve tracking of sources, the NRC has been developing a National Source Tracking System (NSTS), as required by the Energy Policy Act of 2005. The NSTS is one of the most important initiatives at the NRC. Its design will allow the NRC and, in a later release, State and other Federal agencies to track transactions involving the higher risk radioactive sources from origin through transfer to disposition thereby reducing the chance of malicious use by terrorists.

NSTS development has been difficult because of the need to ensure adequate cyber security to protect the database from unauthorized access. The NRC has made considerable progress and currently plans to deploy the NSTS by December 2008. These plans depend on the system passing mandatory systems security testing, and receiving an authority to operate. The NRC has categorized NSTS as a "high" system, meaning that confidentiality, integrity, and availability requirements are all categorized as high impact. By categorizing NSTS as high, the NRC is committed to implementing the system with the most stringent set of controls and a very strong security architecture. NSTS will be the NRC's first system to be implemented at this level. Authentication of the NSTS application requires that each user have an NRC-issued digital certificate on a separate hard token to gain access to the system.

FISMA Compliance

The NRC recognizes the importance of providing an overarching, effective information security program that complies with FISMA, as well as OMB and NIST guidance. This program must ensure the effectiveness of security controls over information resources and assets, and provide for development and maintenance of controls required to protect our systems and information.

In September 2007, the NRC Inspector General identified two significant deficiencies: a lack of current certification and accreditation for most of the agency's systems and a lack of annual contingency plan testing was not performed for all systems. The NRC declared the Information Security Program as a material weakness.

Over the succeeding months, the NRC has taken aggressive action to strengthen our IT security program across a broad range of activities. These include the following:

- Establishing and staffing the CSO to be run by a Chief Information Security Officer, who reports directly to me. The new Chief Information Security Officer, Patrick Howard, will join the NRC next week. Mr. Howard was most recently the Chief Information Security Officer for the Department of Housing and Urban Development (HUD). Mr. Howard has a strong background in FISMA and law enforcement, a superb record working with Federal agencies such as HUD and the Department of Transportation, and was instrumental in helping both of these agencies address serious FISMA deficiencies.
- Certifying and accrediting 12 systems since April 2007, representing 32 percent of the 37 major applications and general support systems. The NRC plans to certify and accredit 10 additional systems by June of 2008 and expects that all remaining systems will be certified and accredited by the end of FY 2009.

- Continuing to mature the certification and accreditation process through improved quality assurance activities and independent evaluations.
- Increasing the number of systems that have been categorized using NIST standards.
- Consolidating systems within our inventory and, where possible, modernizing legacy applications sooner.
- Requiring that tests of system contingency plans be conducted by the end of June 2008, and linking the requirement to Senior Executives' performance.

Certification and Accreditation Improvements

In the October 2007 report to OMB, the NRC Inspector General rated the NRC's Certification and Accreditation process as failing. This is due in large part to the very small number of accredited systems at the time of the audit. As referenced above, the agency has made progress during the last eleven months. To facilitate the process, we have hired additional staff to lead the Certification and Accreditation activities, and increased utilizing contractor support to supplement several accreditation activities. Further, we are constantly challenging ourselves to identify additional actions to increase efficiency. An example of this is the NRC's use of the Environmental Protection Agency's ASSERT tool starting in April 2008, which will automate our Certification and Accreditation process. The tool facilitates the development of security requirements and documentation, allows for reuse of security information as it flows through the Certification and Accreditation process, and allows close oversight and tracking of security control testing and implementation status. We believe that these efforts will expedite the Certification and Accreditation process and allow NRC to be fully compliant with NIST standards.

Another important aspect is that the NRC has focused efforts on the Certification and Accreditation of those information systems that are a high priority from a mission perspective and/or those that potentially pose a higher security risk, regardless of whether the system is new or is a legacy system.

Independent Assessment of the NRC Security Program

The NRC utilized outside expertise under contract to perform an independent review and evaluation of our Certification and Accreditation process. The purpose of this contract was to assess the direction the NRC is taking with its information security, better understand effective practices used elsewhere in the Federal government, and identify long-term improvements for Certification and Accreditation of NRC information systems. The NRC utilized Carnegie Mellon University's Software Engineering Institute (SEI), a Federally Funded Research and Development Center (FFRDC) and recognized leader in cyber-security and assessment methodology, to conduct the independent review. Staff from the SEI's CERT Program led the independent review. The independent review looked at the NRC's approach to FISMA compliance and protecting sensitive information. Specifically, this independent review:

- Evaluated the Certification and Accreditation process' compliance with FISMA and its adherence to NIST guidance;
- Reviewed the risk assessment process and risk management principles used in executing the Certification and Accreditation process;
- Determined if the resource commitment to Certification and Accreditation (funding and effort) is reasonable and appropriate; and

- Evaluated the contribution of Certification and Accreditation activities to the overall security posture of the NRC mission and supporting information systems.

The NRC also tasked SEI to conduct a benchmark assessment to compare the NRC's IT Security Program and Certification and Accreditation process to the practices of other Federal agencies. The review compared the current state of compliance with FISMA requirements with respect to percent of systems accredited, as well as the quality of documentation and the level of conservatism in the security controls implemented. The review also compared the cost of accrediting systems and the process used for certification and accreditation with the costs and best practices at the other agencies. The review concluded in January 2008, and identified opportunities for further improvement and acceleration of our Certification and Accreditation, many of which are currently underway.

IT Security Training

The NRC recognizes the importance of providing staff the information security training necessary to carry out their assigned duties effectively. Rapid technology changes make it necessary to constantly refresh the skills and expertise of employees to keep pace with the changes. To date, NRC has provided comprehensive information security awareness and general security training to all employees. Staff members with information security responsibilities also need role-specific training to enable them to fulfill their security responsibilities as information security practices and requirements change.

As a result of our comprehensive training, the NRC's costs for information security training are higher than training costs at other agencies. In FY 2007, NRC delivered and required all NRC staff to take classroom information systems security awareness training course for general users. The agency believed that it was important to sponsor an in-person class to ensure that the users fully understood their role in the organization's Information Security Program. The students were afforded opportunities to interact with instructors and have their concerns and questions answered and addressed.

The NRC annually updates its on-line Security Awareness Training Course for general users. The updated course will be available this month. Additionally, the NRC updates its security awareness courses for Information System Security Officers and System Administrators every three years. The next version of these courses will be delivered this summer.

The NRC plans to enter into an agreement with the Department of State in FY 2008 to ensure that NRC staff receives current, relevant, and consistent information security training. The agreement will allow the NRC to utilize the Department of State's services to meet NRC information security training needs. This agreement will be executed under the auspices of the Federal Information Systems Security Line of Business initiative. The Department of State's training will provide in-person training to Information System Security Officers and Executives. These courses will be customized to NRC's environment and processes so individuals will have a clear understanding of their roles and the responsibilities. In FY 2009, additional courses for Systems Owners and Managers with significant information security responsibilities will be offered. In FY 2010, additional courses will be offered to Windows-based and Linux/Unix-based administrators.

Additionally, the NRC is considering moving from an NRC-provided course for General User Security Awareness to a course provided by the Department of Defense, also under the auspices of the Information Systems Security Line of Business. Some customization of this course will be necessary because of NRC's use of Safeguards Information. The NRC plans to utilize the Department of Defense's course in FY 2009.

Finally, the NRC is sponsoring classes through Microsoft to enhance the technical skills and security knowledge of our Windows-based administrators. The first class was held in January 2008. The class focused on Securing Microsoft Windows 2003 Servers Defense in Depth. Another class is scheduled for late summer 2008 on Microsoft's Active Directory.

Thoughts about FISMA – Strengths and Weaknesses

Despite the challenges facing the NRC, the NRC remains firmly committed to meeting the standards and requirements of FISMA. I believe that among its strengths, FISMA has established a solid framework for an agency-wide IT security program and for the implementation of necessary system security controls. FISMA establishes accountability for information security. The agency head and Chief Information Officer are assigned specific information security responsibilities. FISMA also requires agencies to establish the position of Chief Information Security Officer (or senior agency information security officer). Over the last couple of years, FISMA has also led to a higher level of standardization in information security programs, terminology, policies, and practices across government, which has facilitated establishment of a higher degree of trust between agencies. This is vitally important.

Nonetheless, I believe improvement is needed. FISMA compliance as currently measured does not permit an accurate view of the effectiveness of its implementation because metrics concentrate on development of plans, policies and procedures, and the implementation of controls. These metrics assume that all controls are of equal weight and importance. In practice, this is not true. For instance, FISMA reporting could be adjusted to include a requirement to report on agency controls to prevent data leaks. Furthermore, reporting should give greater weight to the implementation of controls that defend against high impact threats and that counter the most significant vulnerabilities.

I believe that FISMA requirements are sufficiently comprehensive and flexible to permit an agency to balance compliance requirements against overall needs for security. However, over-emphasis on the annual FISMA report card does not allow for a clear picture of the relative security posture of agencies, (e.g., the expanse and complexity of agency information technology infrastructures, size of user populations, and criticality of agency missions). Implementing security that aims to simply satisfy FISMA reporting requirements will not necessarily lead to an effective information security program. There have been instances of "A" agencies suffering significant data breaches and PII "spills." This occurs because agencies are not required to report specifically on actions they are taking to prevent or minimize the opportunity for such incidents. Additionally, the occurrence of security incidents and violations is not factored into annual compliance scoring.

Finally, the role of the Inspectors General cannot be understated. My experiences with the Inspector General, both here and at my previous agencies, despite the audit findings, have been positive. Those with whom I have worked generally have performed accurate, fair assessments of the quality of agency information security programs and activities. The findings and recommendations have only helped to mature the information security programs over time. My only suggestion is that Inspectors General should be provided tools for objectively performing this important evaluation consistently across the Federal government.

Conclusion

In summary, I reiterate that the NRC is diligently working to ensure secure systems. Executive management at the highest levels of the agency has taken responsibility for the security of NRC's information systems and FISMA compliance. The NRC is taking strong and deliberate steps to build a sound information security program to address the security of NRC's information systems and correct FISMA compliance shortfalls. My goal is to provide an effective security program that weighs risk, openness, and cost as an institutionalized part of NRC business practices in support of NRC's mission to ensure adequate protection of public health and safety, to promote the common defense and security, and to protect the environment.

Again, I thank you for the opportunity to comment on this important topic and I look forward to answering any questions that you may have.