NRC STAFF COMMENTS ON THE OIG ANNUAL FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) REPORT FOR FY 2006

The NRC fully supports the requirements for FISMA compliance and believes these activities are essential to protecting the information and resources the agency uses to carry out its mission. NRC systems will be accredited when all appropriate risk-based information technology (IT) security controls are implemented, operating as intended, and produce the desired result. NRC recognized the need to bring better focus to IT security and in July 2005 developed a plan to implement an information system security (ISS) program that ensured a more comprehensive plan for IT system security. That plan was provided to the NRC Commission on July 21, 2005. The plan included early implementation of Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems, that resulted in an early impact to NRC system certification and accreditation (C&A). However, planning ahead for implementation of these standards poised NRC to be compliant earlier than would otherwise be possible. The plan was accepted by the Commission in December 2005.

The NRC is also taking aggressive and deliberate steps to continue building a sound ISS Program to address the security of NRC's information systems and FISMA compliance shortfalls. Our goal is to provide an effective security program that weighs risk, openness, and cost as an institutionalized part of everyday business practices.

Although the NRC agrees with the majority of the OIG findings, it is important to note that significant work has continued beyond August, 2006. The NRC will: 1) complete security categorizations for all major and general support systems by the end of calendar year 2006 and 2) complete the certification and authorization of six of the systems that are of highest mission priority by the end of January, 2007.

NRC is taking a proactive role in ensuring compliance with new FISMA guidance. NRC is carefully and deliberately building a sound ISS program in a fiscally responsible fashion. In particular, NRC is using NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems and the new NIST SP 800-53, Recommended Security Controls for Federal Information Systems for all NRC major systems to ensure full compliance as soon as possible. However, the NIST SP 800-53 introduced a level of detail and granularity that is significantly greater than what was contained in previous guidance. The review of existing security documentation during the C&A process found that many NRC systems did not contain the level of detail necessary to address the security control requirements of NIST SP 800-53 without significant revision, and system development methodologies did not deliver system and security documentation with the appropriate level of detail required for C&A.

Compliance in a fiscally responsible manner requires establishing standardized security controls for information systems and developing verification procedures for assessing the effectiveness of those controls, as well as effective integration of security C&A with system development processes and more effective delivery of required security documentation and products. The effort to move toward corporate management of IT and identification of common IT security controls and products to support NRC systems has caused a delay in full system C&A of many NRC systems, particularly legacy systems. However, this proactive approach will ultimately simplify both system development activities and system operations and maintenance while ensuring IT security and full and complete system C&A for all NRC major systems. NRC has focused its efforts on the C&A 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. NRC has made significant progress toward FISMA compliance in FY 2006.

NRC has reviewed existing internal practices to identify opportunities to streamline and automate the system C&A process and better integrate the security and system development processes. Modifications to the practices will enable more effective delivery of required security documentation and products, consistent implementation of OMB and NIST guidance, flexible and scalable security processes, and version control and configuration management for all security documentation. NRC is automating our C&A process through the use of an automated tool suite that will facilitate the development of security requirements and documentation, allow for reuse of security information as it flows through the C&A process, and allow close oversight and tracking of security control testing and implementation status. These tools allow integration of agency enterprise architecture, system development, and security processes. NRC has documented the C&A process and the process is available across the agency via an internal web page.

NRC engaged an outside independent contractor to perform an independent review and evaluation of its information assurance C&A process to assess the effectiveness of the NRC ISS Program, better understand effective practices used elsewhere in the Federal government, and identify long-term solutions for the C&A of NRC information systems. NRC has also tasked the independent contractor to conduct a benchmark to compare NRC’s ISS Program and C&A process to the practices of two other Federal agencies. The review compares 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 compares the cost of accrediting systems and the process used for C&A with the costs and best practices at the other agencies. The independent review reports will be completed in first quarter FY 2007.

In December 2005, the NRC engaged an outside contractor to conduct an external and internal IT security penetration test against the agency. The purpose of this test was to understand the external presence of the NRC on the Internet, identify security vulnerabilities that could be taken advantage of by hackers over the Internet, identify internal threat sources, assess NRC’s compliance with documented policies and procedures, and develop recommendations for fixing and/or addressing vulnerabilities that could be exploited.

The results of the penetration testing identified strong perimeter security practices through deployment of external security measures and controls currently in place. The contractor was unable to obtain a full network mapping of NRC computers, servers, and devices from an external Internet connection due to preventive measures the agency has implemented. The testing identified a number of internal security vulnerabilities, such as network ports not adequately protected, the ability to obtain user network Identifications and passwords through social engineering techniques, and the willingness of staff to provide access to workstations through responses to bogus e-mails. As a follow-on effort, penetration tests were also performed at each NRC regional office and NRC's Technical Training Center during July 2006. Identification of issues from the penetration testing is enabling NRC to address the most significant IT security concerns and take immediate corrective actions. As a result of the social engineering vulnerabilities, NRC has developed in-person IT security training for all NRC users in addition to NRC's annual on-line awareness course. The course is mandatory and will be conducted during the first and second quarters of FY 2007.

NRC has also begun to implement quarterly operating system scans. These scans reveal issues that make systems vulnerable to both external and internal attacks. In order to address some of the most significant issues identified during the scans, NRC has implemented Patchlink. Patchlink enables NRC to push patches out to systems that reside within NRC's infrastructure and enables a much faster implementation of critical IT security patches.

NRC efforts to hire and retain staff resources with the necessary IT security skills has been challenging. In order to complete NRC system C&A the agency has awarded a contract to provide C&A and FISMA support services consistently across the agency. This contract was awarded at the end of July 2006.

NRC has prioritized the C&A of systems based upon the criticality of the systems to NRC's mission. The highest priority systems are being addressed first and most of those systems have completed the security categorization process, the e-authentication risk analyses, and the risk assessment. During the security categorization process, many system owners characterized their systems as having a higher sensitivity than corresponds to federal guidance. NRC brought the sensitivity in line with federal guidance to ensure adequate risk-based IT security controls and thus avoided the significant cost of implementing the IT security controls for a higher sensitivity level. Based upon the risk assessments, NRC is taking corrective action prior to completing the system security plans.

Where NRC relies on another government agency for system services, NRC has made every attempt to review the system C&A documentation and ensure the system is providing adequate IT security controls for the NRC information being processed. In some cases, this has not always been possible.

NRC has made significant strides during FY 2006 to ensure that NRC information and information systems are appropriately secured and to ensure NRC FISMA compliance. The work completed to date, particularly completion of the security categorization, has given us confidence that our understanding of systems is fairly accurate, even though the documentation has not been completed. All efforts have been risk-based and consistent across all NRC systems. NRC believes that with the recently acquired additional contractor resources, NRC will be able to make even more progress over FY 2007.