"NRC Report on the Implementation of the Federal Information Security Management Act For Fiscal Year 2003"

Prepared by the NRC Chief Information Officer

September 15, 2003

A. OVERVIEW OF FISMA IT SECURITY REVIEWS

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.

Bureau Name	FY03 IT Security Spending ($ in thousands)
United States Nuclear Regulatory Commission (NRC) The NRC has only one major operating unit. Also, the NRC does not have any critical infrastructure, and thus has no critical infrastructure protection costs	$3,379
Agency Total	$3,379

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.

	FY03 Programs		FY03 Systems		FY03 Contractor Operations or Facilities	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Total Agency (NRC has no bureaus)	1	1	20	20	7	7
Agency Total	1	1	20	20	7	7
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	**Yes**			**Yes**		
c. If yes, what methods are used? If no, please explain why.	The NRC utilized the applicable sections of the NIST self assessment guide in conducting reviews of contractor provided services and reviews of the services provided by other agencies. The NRC also used the National Security Agency's (NSA) INFOSEC Assessment Methodology (IAM) in completing a security review of one NRC contract. The NRC has Memorandums of Agreement (MOAs) in place with two other government agencies for IT services. These agencies are the National Institute of Health (NIH), and the Department of Interior. Both agencies have completed GISRA/FISMA annual reviews and have current corrective action plans in place. NRC has discussed the results of the GISRA/FISMA reviews completed by these other agencies. (Both agencies refused to allow NRC to conduct its own separate review).					
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	**Yes**			**Yes**		
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	**N/A**			The NSA IAM contains all the elements of NIST's self assessment guide.		
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.	NRC has an inventory in place for its major IT systems as part of the Enterprise Architecture work.					

NRC National Security Programs and Systems

NRC is not the system owner for any applications or systems that process classified national security information. However, NRC is a subscriber to several classified applications, such as AUTODIN and INTEL LINK. All of these applications are operated and maintained in approved Secure Compartmented Intelligence Facilities (SCIF) at NRC. Coordination was accomplished in past years with the system owners for several classified systems and authorizations were obtained leading to the installation of single terminal drops for each of the classified systems. In some instances terminals were provided by the external system owners that would enable NRC to dial in remotely to a classified system that is owned and maintained by the external organizations. In each case, the system owners verified that NRC had adequate security protections in place before an NRC terminal drop or connection was authorized. Periodic security inspections or reviews are conducted of NRC classified operations and facilities by the system owners, although these are infrequent. In accordance with the FISMA guidance, the NRC conducted security reviews for all of our classified systems. While no specific guidance was provided by the intelligence community, the National Security Agency, or the Department of Defense, for how to conduct security reviews for subscriber installations such as NRC, the NRC computer security staff utilized the Department of Defense Information Assurance Readiness Review (IARR) process in conducting security reviews of our classified subscriber systems. The IARR guidance addresses all elements that are contained in the NIST Self Assessment guidance. Some tailoring of the IARR process was required as several sections were specific to the Defense Department and not applicable to NRC. The security reviews did not identify any security weaknesses that needed to be included in the agency POA&M. One principal reason is that these classified subscriber terminals and systems are all located in approved NRC SCIF environments, which have the highest levels of security protections. NRC intends to work with the system owners at the external organizations and seek additional guidance in conducting future FISMA security reviews in FY 2004.

Since September 11th, 2001, the NRC has experienced increasing requirements for the processing of sensitive and classified national security information. NRC has utilized stand alone desktop computer workstations and laptop computers in several different NRC office spaces to process classified information, recognizing that this is not the most optimum approach for processing classified information. NRC is currently assessing our classified information processing requirements, and planning has started to address providing more robust capabilities, (such as classified networks and classified document processing applications). The plans and projects to enhance NRC classified processing capabilities will be initiated in FY2004.

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Total Agency (NRC has no bureaus)	0	0		
Agency Total	0	0		

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	Yes	No
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.		
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.		
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		

B. RESPONSIBILITIES OF AGENCY HEAD

For the purposes of this report, NRC's agency head is the Executive Director for Operations (EDO).

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	As required by FISMA, the agency head (Executive Director for Operations, (EDO)), has tasked the Chief Information Officer (CIO) with the responsibility for managing the agency-wide automated information security program, on behalf of the EDO. Also, the CIO has tasked the Senior Information Technology Security Officer (SITSO) with exercising day to day management and oversight of the program. These responsibilities and authorities, and the responsibilities of all other senior agency officials have all been specified in the agency-wide automated information security program management directive, (MD 12.5). The MD 12.5 has recently been revised to specifically include the FISMA responsibilities and authorities for all agency officials. (The revised MD 12.5 is in the final steps of the agency coordination process). The agency head and CIO conduct reviews of the agency program and individual systems, as the quarterly corrective plan of action and milestone (POA&M) reports are submitted to OMB each quarter. The agency head and the CIO focus on the performance measures for the program, and monthly progress reports are filed with each NRC office to ensure that all requirements of the NRC automated information security program are being implemented and enforced. The agency head and the CIO focus on the performance measures for the program, and monthly progress reports are filed with each NRC office to ensure that all requirements of the NRC automated information security program are being implemented and enforced.
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	No. This policy is enforced through the agency capital planning and investment control (CPIC) process.
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	The agency head and the CIO utilize a central tracking system to track all system information such as the status of security plans, security testing, system weaknesses and corrective actions, and all other security activities associated with systems security certification and accreditation. The agency head and the CIO ensure that new systems cannot be placed into operation, and major system upgrades cannot be completed, until they have completed the security activities

	and milestones required to attain system security accreditation.
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.	The agency head reviews the quarterly corrective plan of action and milestone (POA&M) reports that are submitted to OMB. For any system that may be behind schedule, the agency head initiates action to ensure that the CIO and other senior agency officials have effective action plans in place to resolve any systems security life cycle weaknesses or discrepancies.
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.	The agency does not have mission-critical systems in the sense of PDD 63. The NRC has a current Critical Infrastructure Protection (CIP) Plan and a current Continuity of Operations (COOP) Plan in place. The agency-wide information technology security program requires that all major applications and systems have IT contingency (business continuity) plans in place, and also requires that the plans be tested annually. The agency COOP and CIP Plans also include provisions for maintaining business continuity plans for systems that support its essential functions. In this way the agency effectively integrates critical infrastructure protection responsibilities with the overall security required to enable the NRC to fulfill its most important functions in the event of major disruption from any cause.
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	The Nuclear Regulatory Commission (NRC) has a comprehensive and integrated security program. NRC's security program is documented in six policy directives and handbooks that constitute Volume 12 of the NRC management directive (MD) series, and is consistent with Government-wide laws, regulations, policies, and procedures. NRC MD 12.3, NRC Personnel Security Program, provides for a Government-operated background screening program applicable to all NRC employees and contractors commensurate with their level of access to NRC sensitive automated information systems and data. NRC MD 12.1 covers facility security. The requirements for the NRC Automated Information Security Program are documented in NRC Management Directive 12.5 (NRC Automated Information Security Program). MD 12.5 specifies the roles of each of the NRC organizational elements that contribute to the operation of a single, integrated NRC Automated Information Security Program, managed by the CIO and the SITSO.

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	**X Yes**		No	
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	**X Yes**		No	
c. Has the agency fully identified its mission critical operations and assets?	**X Yes**		No	
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	**X Yes**		No	

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.	
e. If yes, describe the steps the agency has taken as a result of the review.	NRC initiated a Project Matrix review in FY 2002 to provide additional insight into its critical assets and how they are protected. NRC completed the infrastructure asset evaluation (IAE) phase of the review. In working with the Project Matrix Program Office at the Department of Commerce (DOC) in FY 2002, the NRC demonstrated the review process that NRC utilized to review all agency missions, functions and assets. The result of the internal comprehensive review completed in FY 2002 indicated that NRC does not have any nationally critical operations and assets, and NRC does not have any mission critical operations and assets. NRC continued the Project Matrix review process in early FY 2003, in order to independently validate NRC's critical infrastructure assessment process. However, the Project Matrix process has been delayed due to the shifting of the Project Matrix Program from the DOC to the new Department of Homeland Security. As a result of the NRC reviews of our operations and assets, the NRC developed (and updated in FY 2003), the agency COOP Plan and the CIP Plan. Current IT contingency (business continuity) plans are in place for agency major applications and general support systems, and the plans are tested annually.
f. If no, please explain why.	

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?	
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	In FY03, NRC maintained information systems security incident response procedures that ensure that potential security incidents are reported and resolved effectively with appropriate escalation to various management levels. These procedures were reviewed and approved by FedCIRC staff. NRC has a Computer Security Incident Response Capability (CSIRC), which is a team composed of highly skilled technical staff that responds to reported security incidents. The CSIRC also prepares monthly reports that are forwarded up the NRC chain of command, for further forwarding to the FedCIRC. The NRC has a reporting relationship with the FedCIRC, and we report security incidents and share information regarding common vulnerabilities. The NRC information systems security incident response procedures also identify the procedures for external reporting to the appropriate law enforcement authorities. The CSIRC team coordinates with the NRC Office of Inspector General for all incidents that may require assistance or involvement of law enforcement authorities. There have been no successful attacks against NRC automated information systems. NRC has been collecting information systems security incident statistics since FY-2001. The number of incidents detected in FY-2003 is significantly higher than in prior years. Such incidents are typically nuisance level scans that are stopped by NRC first line security measures such as a the NRC firewall or anti-virus software, and no further action is required. The event is logged and included in monthly statistics. NRC will continue to take the aggressive actions necessary to take the incident response procedures a core element of the NRC AIS Security Program.
b. Total number of agency components or bureaus.	1
c. Number of agency components with incident handling and response capability.	1

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
d. Number of agency components that report to FedCIRC.	1			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	**Yes**			
f. What is the required average time to report to the agency and FedCIRC following an incident?	The NRC files monthly status reports to FedCIRC. The NRC did not have any major security incidents that required immediate reporting to FedCIRC, and thus we have no data on average time to report.			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	The NRC updated its patch management policy guidance in FY 2003. The process is managed by the network infrastructure security team, working closely with the systems administrators for all NRC systems. Critical patches that have been identified by FedCIRC are installed in a timely manner, and the network infrastructure ISSO confirms that systems administrators have installed the patches.			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	**X Yes**		No	
i. If yes, how many active users does the agency have for this service?	Currently only 1. Coordination is underway with FedCIRC to expand NRC use of this FedCIRC service.			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	**X Yes**		No	
k. Do these configuration requirements address patching of security vulnerabilities?	**X Yes**		No	

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.

Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement
NRC	67,626	67,626	0

C. RESPONSIBILITIES OF AGENCY PROGRAM OFFICIALS AND AGENCY CHIEF INFORMATION OFFICERS

For the purposes of this report, NRC program officials are the system owners.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
NRC	20	20	100	18	90	18	90	20	100	18	90	18	90	17	85

Agency Total	20	20	100	18	90	18	90	20	100	18	90	18	90	17	85

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
Y	**Y**	The CIO maintains a centralized tracking system to track the status of all agency systems, and the status of all corrective actions. The agency corrective action POA&M is the primary mechanism used to provide management and oversight of the agency-wide IT security program.	**Y**	**Y**

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?

Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
3,188	3,078	96%	33	255	100%	During FY 2003, new staff were provided initial awareness training, all staff were provided refresher awareness training, and those with specific security responsibilities (such as the Information Systems Security Officers formally appointed for each of the applications and systems) were provided role-based training. NRC's security tracking system shows that over 90 percent of NRC staff have received appropriate awareness training, that all Information Systems Security Officers have taken the NRC online ISSO course, and that System Administrators and others who want to expand their knowledge of security are continuing to avail themselves of this training resource.	$40K

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?

Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
NRC	12	Yes	Yes	Yes