Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: Nuclear Regulatory Commission

Question 1 and 2

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
1) Continue to use NIST Special Publication 800-26, or,
2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency, therefore, self reporting by contractors does not meet the requirements of law. Self reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the following: have a current certification and accreditation, a contingency plan tested within the past year, and security controls tested within the past year.

		Question 1						**Question 2**					
		a. Agency Systems		**b. Contractor Systems**		**c. Total Number of Systems**		**a. Number of systems certified and accredited**		**b. Number of systems for which security controls have been tested and evaluated in the last year**		**c. Number of systems for which contingency plans have been tested in accordance with policy and guidance**	
Bureau Name	**FIPS 199 Risk Impact Level**	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
NRC	High	3	0	0	0	3	0	0	0.0%	3	0.0%	0	0.0%
	Moderate	8	0	0	0	8	0	0	0.0%	8	0.0%	3	0.0%
	Low	0	0	1	0	1	0	0	0.0%	1	0.0%	1	0.0%
	Not Categorized	19	0	11	0	30	0	5	0.0%	21	0.0%	0	0.0%
	Sub-total	**30**	**0**	**12**	**0**	**42**	**0**	**5**	**0.0%**	**33**	**0.0%**	**4**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%

	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Bureau	High					0	0		0.0%		0.0%		0.0%
	Moderate					0	0		0.0%		0.0%		0.0%
	Low					0	0		0.0%		0.0%		0.0%
	Not Categorized					0	0		0.0%		0.0%		0.0%
	Sub-total	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0.0%**	**0**	**0.0%**	**0**	**0.0%**
Agency Totals	**High**	**3**	**0**	**0**	**0**	**3**	**0**	**0**	0.0%	**3**	0.0%	**0**	0.0%
	Moderate	**8**	**0**	**0**	**0**	**8**	**0**	**0**	0.0%	**8**	0.0%	**3**	0.0%
	Low	**0**	**0**	**1**	**0**	**1**	**0**	**0**	0.0%	**1**	0.0%	**1**	0.0%
	Not Categorized	**19**	**0**	**11**	**0**	**30**	**0**	**5**	0.0%	**21**	0.0%	**0**	0.0%
	Total	**30**	**0**	**12**	**0**	**42**	**0**	**5**	0.0%	**33**	0.0%	**4**	0.0%

Question 3		
In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.		
3.a.	The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy. Self-reporting of NIST Special Publication 800-26 and/or NIST 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient. Response Categories: - Rarely, for example, approximately 0-50% of the time - Sometimes, for example, approximately 51-70% of the time - Frequently, for example, approximately 71-80% of the time - Mostly, for example, approximately 81-95% of the time - Almost Always, for example, approximately 96-100% of the time	- Mostly, for example, approximately 81-95% of the time
3.b.1.	The agency has developed an inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency. Response Categories: - Approximately 0-50% complete - Approximately 51-70% complete - Approximately 71-80% complete - Approximately 81-95% complete - Approximately 96-100% complete	- Approximately 51-70% complete
3.b.2.	If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.	Missing Agency Systems: Network Continuity of Operations Missing Contractor Systems:
3.c.	The OIG **generally** agrees with the CIO on the number of agency owned systems.	Yes
3.d.	The OIG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency.	Yes
3.e.	The agency inventory is maintained and updated at least annually.	Yes
3.f.	The agency has completed system e-authentication risk assessments.	No

Question 4

Through this question, and in the format provided below, assess whether the agency has developed, implemented, and is managing an agency wide plan of action and milestone (POA&M) process. Evaluate the degree to which the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

For items 4a.-4.f, the response categories are as follows:

- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

4.a.	The POA&M is an agency wide process, incorporating all known IT security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.	- Almost Always, for example, approximately 96-100% of the time
4.b.	When an IT security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).	- Almost Always, for example, approximately 96-100% of the time
4.c.	Program officials, including contractors, report to the CIO on a regular basis (at least quarterly) on their remediation progress.	- Almost Always, for example, approximately 96-100% of the time
4.d.	CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.	- Almost Always, for example, approximately 96-100% of the time
4.e.	OIG findings are incorporated into the POA&M process.	- Almost Always, for example, approximately 96-100% of the time
4.f.	POA&M process prioritizes IT security weaknesses to help ensure significant IT security weaknesses are addressed in a timely manner and receive appropriate resources	- Almost Always, for example, approximately 96-100% of the time

Comments: NRC has two primary tools for tracking IT security weaknesses. At a high level, NRC uses the POA&Ms submitted to OMB to track (1) corrective actions from the OIG annual independent evaluation, (2) corrective actions from the agency's annual review, and (3) recurring FISMA and IT security action items such as annual self-assessments, and annual contingency plan testing. The POA&Ms may also include corrective actions resulting from other security studies conducted by or on behalf of NRC. At a more detailed level, NRC uses an internal system to track the progress of more specific corrective actions. These include corrective actions resulting from activities associated with the certification and accreditation process (e.g., risk assessment, security test and evaluation).

Question 5	
OIG Assessment of the Certification and Accreditation Process. OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May, 2004) for certification and accreditation work initiated after May, 2004. This includes use of the FIPS 199 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.	
Assess the overall quality of the Department's certification and accreditation process. Response Categories: - Excellent - Good - Satisfactory - Poor - Failing	- Failing
Comments: See attached narrative, page 4.	

Section C: Inspector General. Questions 1, 2, 3, 4, and 5.

Agency Name: Nuclear Regulatory Commission

Question 6

6.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
	Comments:	

6.b. Configuration guides are available for the products listed below. Identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

Product	**Addressed in agencywide policy?** **Yes, No, or N/A.**	**Do any agency systems run this software?** **Yes or No.**	**Approximate the extent of implementation of the security configuration policy on the systems running the software.** **Response choices include:** **- Rarely, or, on approximately 0-50% of the systems running this software** **- Sometimes, or on approximately 51-70% of the systems running this software** **- Frequently, or on approximately 71-80% of the systems running this software** **- Mostly, or on approximately 81-95% of the systems running this software** **- Almost Always, or on approximately 96-100% of the systems running this software**
Windows XP Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows NT	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Professional	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2000 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Windows 2003 Server	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Solaris	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software

HP-UX	No	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Linux	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Cisco Router IOS	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Oracle	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Other. Specify: Novell, AIX, Sybase, SQL Server, Cisco PIX, IIS, Apache	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software

Comments: W2K Pro is installed only on selected standalone laptops purchased when W2K Pro was the standard Microsoft operating system. These systems are not part of the NRC production operating environment (POE). HP-UX is found in the production environment, but it is not in widespread use and there is no baseline. Oracle configuration guides are available, but this software is currently not in production. Oracle is being tested for planned future production use. Apache configuration guides are also available, but this software is only found in the POE as a customized version that is bundled with the list manager for the Web interface. It is also installed on a development server. IIS hardening guidelines are included in the Windows 2000/2003 configuration guides. There is an IIS 5 configuration guide.

Question 7		
Indicate whether or not the following policies and procedures are in place at your agency. If appropriate or necessary, include comments in the area provided below.		
7.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
7.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
7.c.	The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.	Yes
Comments:		

Question 8		
8	Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Response Choices include: - Rarely, or, approximately 0-50% of employees have sufficient training - Sometimes, or approximately 51-70% of employees have sufficient training - Frequently, or approximately 71-80% of employees have sufficient training - Mostly, or approximately 81-95% of employees have sufficient training - Almost Always, or approximately 96-100% of employees have sufficient training	- Mostly, or approximately 81-95% of employees have sufficient training

Question 9		
9	Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency wide training? Yes or No.	Yes

NRC's Implementation of FISMA for FY 2006
Additional Narrative for Section C: OMB FISMA Reporting Template for Agency IGs

The following supplemental information is provided in support of the FY 2006 Office of Management and Budget (OMB) Federal Information Security Management Act (FISMA) Reporting Template for Agency Inspectors General for the Nuclear Regulatory Commission (NRC). The independent evaluation of NRC's implementation of FISMA for FY 2006 was conducted by Richard S. Carson and Associates, Inc. (Carson Associates) on the behalf of the NRC Office of the Inspector General (OIG).

Question 1a. NRC has a total of 30[1] operational systems that fall under FISMA reporting requirements. [2] Of the 30, 17 are general support systems, and 13 are major applications. As required by FISMA, the NRC OIG selected a subset of NRC systems for evaluation during the FY 2006 FISMA independent evaluation. However, during the course of fieldwork, the OIG learned that the re-certification and re-accreditation of these systems, scheduled to be completed by August 2006, would not be completed during the FY 2006 FISMA reporting period. Furthermore, there were no other systems to evaluate because there were only two operational systems with a current certification and accreditation at the time the OIG was selecting systems for evaluation. One of these systems was evaluated by the OIG in FY 2006 and the other system's certification and accreditation expired during the FY 2006 FISMA reporting period. Without enough systems with current certifications and accreditations, Carson Associates could not perform an evaluation of a representative subset of agency systems for the FY 2006 FISMA independent evaluation.

Question 1.b. NRC has a total of 12 systems operated by a contractor or other organization on behalf of the agency (8 major applications and 4 general support systems). Of the 12, 7 are operated by other Federal agencies, 2 are operated by federally funded research and development centers, and 3 are operated by private contractors. Carson Associates selected 1 of the 12 systems operated by a contractor or other organization on behalf of the agency for evaluation during the FY 2006 FISMA independent evaluation. However, that system did not have a current certification and accreditation and there was not sufficient information available to perform an evaluation.

Question 2. The metrics in Question 2 represent the status for all NRC systems, not just a subset of systems.

Question 2.a. Only one agency system is certified and accredited, and only four systems operated by a contractor or other organization on behalf of the agency are certified and

[1] The agency reports 31 operational systems. The OIG disagrees with the agency that an OIG system is a major application. It has been categorized as a listed system since it began operations in 2004. This designation is presently under a detailed review. Therefore, the metrics submitted by the OIG reflect a total of 30 operational systems.

[2] NRC also has a number of major applications and general support systems currently in development. For FISMA reporting purposes, only operational systems are considered.

accredited. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements and that other contractor systems are certified and accredited.

In accordance with OMB requirements, the fact that only 1 of the 30 operational NRC information systems has a current certification and accreditation, and that only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation, constitutes a ***significant deficiency***.

Question 2.b. NRC meets the FISMA requirement to test and evaluate the security controls of agency information system by performing annual self-assessments on the systems. In addition, NRC developed a self-assessment for common controls that are applicable to all NRC systems. NRC performed self-assessments on all agency operational systems with the exception of one general support system. NRC also performed self-assessments on the four NRC regions and the NRC Technical Training Center.

NRC performed self-assessments on 4 of the 12 systems operated by a contractor or other organization on behalf of the agency. The remaining 8 systems are operated by other Federal agencies. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements.

Question 2.c. Only three agency systems had their contingency plans tested in the last year. The agency has reported that two additional major applications had their contingency plans tested in the past year. However, the testing results for these systems are still under review by the agency. Therefore, those systems are not included in the metrics. The agency has also reported that one contractor system had its contingency plan tested in the past year. NRC is still developing procedures for maintaining documentation that demonstrates systems provided by other Federal agencies meet FISMA requirements.

In accordance with OMB requirements, the fact that the agency has failed to conduct annual contingency plan testing for the past two years constitutes a ***significant deficiency***.

Question 3.a. NRC presumes that the Federal agencies that operate 8 of the 12 contractor systems are also following FISMA and guidelines from the National Institute of Standards and Technology (NIST). However, the agency is still implementing recommendations from the FY 2005 FISMA independent evaluation to (1) maintain copies of all certification and accreditation documentation for these systems, (2) verify that the security controls have been tested and evaluated for these systems on an annual basis, and (3) verify that the contingency plans have been tested and evaluated for these systems on an annual basis. The agency has been working with the offices to assist in acquiring the required documentation for the contractor systems provided by other Federal agencies. However, according to the agency, some of the other Federal agencies have been unwilling to provide documentation that demonstrates they meet FISMA requirements. The other Federal agencies have also been unwilling to share copies of their annual self-assessments or results from their annual contingency plan testing. In a follow-up memorandum to the agency regarding the status of these recommendations, the OIG suggested a possible solution to the problem. The OIG stated that a memorandum from the

Federal agencies stating that annual self-assessments and annual contingency plan testing have been completed will be sufficient to meet the intent of the recommendations. The agency is currently working towards obtaining such memoranda.

The agency is also still developing procedures for performing sufficient oversight and evaluation for contractor systems provided by private contractors to ensure the information systems meet requirements of FISMA, OMB policy, NIST guidelines, and agency policy.

Question 3.b.1. While FISMA requires agencies to maintain an inventory of only major information systems (major applications and general support systems), NRC also tracks two other system types in its inventories – Listed[3] and Other.[4] The FY 2005 FISMA independent evaluation found that the agency's inventory was only 51-70 percent completed because (1) information in the agency's two inventory systems was inaccurate and inconsistent and (2) only one of the two inventory systems contained information on system interfaces. In FY 2006, Carson Associates did not evaluate whether the agency inventory included information on system interfaces as the agency has not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

Question 3.b.2. The agency's Network Continuity of Operations system is currently categorized as a listed system. In accordance with OMB guidance, the NRC Network Continuity of Operations system is a high-impact system, and therefore should be categorized as a general support system, and not a listed system.

Question 3.c. Carson Associates generally agreed with the CIO on the number of agency owned major applications and general support systems. However, Carson Associates did not fully evaluate the completeness of the agency's inventory, as the agency has not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

Question 3.e. Carson Associates did not fully evaluate whether the agency inventory is maintained and updated at least annually, as the agency has not completed the recommendations resulting from the FY 2005 FISMA independent evaluation regarding problems with the inventory.

Question 3.f. The FY 2005 FISMA independent evaluation found that e-authentication risk assessments had been completed for only 6 of the agency's 27 operational systems.[5] In FY 2005, Carson Associates reviewed the six completed e-authentication risk assessments and found them to be incorrect and inconsistent with the systems' security categorizations. In FY 2005, the agency stated that e-authentication risk assessments would be "supported under the interim

[3] A Listed system is a computerized information system or application that (1) processes sensitive information requiring additional security protections and (2) may be important to an NRC office's or region's operations, but which is not a major application or general support system when viewed from an agency perspective. Sensitive data may include individual Privacy Act information, law enforcement sensitive information, sensitive contractual and financial information, safeguards, and classified information.

[4] An Other system is an NRC system that does not require additional security protections and is adequately protected by the security provided by the NRC local area network/wide area network.

[5] In FY 2005, the agency had 27 operational systems. The agency now has 30 operational systems.

Information Systems Security contract awarded August 11, 2005 and were expected to be completed by December 15, 2005." However, as of September 1, 2006, the agency had only provided e-authentication risk assessments for 10 of the agency's 30 operational systems, and 1 of the agency's contractor systems.

Question 4. While the agency's POA&M process is adequate, the agency has made minimal progress in correcting weaknesses reported on it POA&Ms. The agency has corrected 15 percent of its program level weaknesses, and 22.7 percent of its system level weaknesses. The majority of delays have been caused by delays in completing certifications and accreditations.

Question 5. To correct weaknesses identified by the FY 2005 FISMA independent evaluation by the NRC OIG, and to address findings from the agency's own evaluation, the agency has refocused its information system security program. Under the refocused program, the agency will first perform certification and accreditation for those systems that are a high priority from a mission perspective, and those that potentially pose a higher security risk (e.g., agency systems that communicate with systems outside the NRC network). The first phase of the refocused program included the development of a comprehensive certification and accreditation process, which is not yet finalized. The agency developed templates for all certification and accreditation documents and instructions for completing the templates. The updated certification and accreditation process was also integrated into the agency's new project management methodology. One of the agency's operational major applications was chosen to "pilot" the new process and documentation standards, in part, to ensure the new process is repeatable.

The refocused program has not resulted in the completion of a single certification and accreditation despite the (1) emphasis on the certification and accreditation of high priority systems and systems with a higher security risk and (2) application of at least $500,000 in funding to this initiative since December 2005. In the meantime, the certifications and accreditations for all but one of the agency's operational systems have expired. The certification and accreditation for the one agency system that was current during the evaluation expires in October 2006.

As stated previously, the fact that only 1 of the 30 operational NRC information systems has a current certification and accreditation, and that only 4 of the 12 systems used or operated by a contractor or other organization on behalf of the agency have a current certification and accreditation, constitutes a ***significant deficiency***.

Question 8. NRC ensures all employees and contractors receive security awareness and training. However, the FY 2005 FISMA independent evaluation found that the agency had difficulty in gathering the information needed to report on (1) the total number of employees with significant IT security responsibilities, (2) the number of those employees who have received specialized training, and (3) the total costs for providing IT training. The agency is still developing procedures for ensuring employees with significant information technology security responsibilities receive security training.