Section B: Chief Information Officer. Questions 1, 2, 3, and 4.

Nuclear Regulatory Commission (NRC)
Date: 9/14/2006

Question 1 and 2

1. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of information systems used or operated by your agency, and the number of information systems used or operated by a contractor of your agency or other organization on behalf of your agency.

Note: Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

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.

FIPS 199, a Federal information processing standard, was published in February 2004. If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain below in item (d.).

2. For each part of this question, identify actual performance for the past fiscal year by risk impact level and bureau, in the format provided below. From the Total Number of Systems, identify the number of systems which have: a current certification and accreditation , a contingency plan tested within the past year, and security controls tested within the past year. Contingency planning is a requirement for certification and accreditation, with annual contingency plan testing required thereafter. If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain.

		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
Bureau	High	3	0	0	0	3	0	0	0.0%	3	100.0%	0	0.0%
	Moderate	8	0	0	2	8	0	0	0.0%	8	100.0%	3	37.5%
	Low	0	0	1	0	1	0	0	0.0%	1	100.0%	1	100.0%
	Not Categorized	20	0	11	0	31	0	5	16.1%	21	67.7%	0	0.0%
	Sub-total	**31**	**0**	**12**	**2**	**43**	**0**	**5**	11.6%	**33**	76.7%	**4**	9.3%
Agency Totals	**High**	**3**	**0**	**0**	**0**	**3**	**0**	**0**	**0.0%**	**3**	**100.0%**	**0**	**0.0%**
	Moderate	**8**	**0**	**0**	**2**	**8**	**0**	**0**	**0.0%**	**8**	**100.0%**	**3**	**37.5%**
	Low	**0**	**0**	**1**	**0**	**1**	**0**	**0**	**0.0%**	**1**	**100.0%**	**1**	**100.0%**
	Not Categorized	**20**	**0**	**11**	**0**	**31**	**0**	**5**	**16.1%**	**21**	**67.7%**	**0**	**0.0%**
	Total	**31**	**0**	**12**	**2**	**43**	**0**	**5**	**11.6%**	**33**	**76.7%**	**4**	**9.3%**

1.d.	If there are systems which have not yet been categorized, or, if a risk impact level was determined through another method, please explain: Unable to accomplish system categorization due to lack of resources. This is a planned activity for FY2007.
2.d.	If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain: System owners of non-categorized systems did not have sufficient resources to update their system's contingency planning process this year.

Question 3

Agencies must implement the recommended security controls in NIST Special Publication 800-53.

3.a.	Do you have a plan in place to fully implement the security controls recommended in NIST Special Publication 800-53? Yes or No.	Yes
3.b.	Have you fully implemented the security controls recommended in NIST Special Publication 800-53? Yes or No	No

Question 4		
Incident Detection Capabilities.		
4.a.	What tools, techniques, technologies, etc., does the agency use for incident detection? The agency uses Snort intrusion detection in several locations to analyze traffic from the internet and critical networks. We run a daily report of all internet activity with thesholds and explain variances. We employ the Symantec and Sophos anti virus and PUP (potentially unwanted programs) protection on Internet email and at the desktop. We have an Agency-wide program for vulnerability notification and patch deployment. We use a multi-level firewall configuration and house all public facing systems in a DMZ isolated from the Internet and our internal networks. We have operating system baselines for most operating systems in use in the Agency and programs to ensure adherence to standards. We proxy network traffic between the Internet and our internal networks and only allow active content from specific trusted sites. We have partially deployed enterprise vulnerability scanning and enterprise automated patching.	
4.b.	How many systems (or networks of systems) are protected using the tools, techniques and technologies described above?	33

Section B: Chief Information Officer. Question 5.
Nuclear Regulatory Commission (NRC)
Date: 9/14/2006

Question 5

Information gathered in this question will be forwarded to the Department of Homeland Security for validation.

For each category of incident listed: identify the total number of successful incidents in FY 05, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category e., "Other". If appropriate or necessary, include comments in the area provided below.

	5. Number of Incidents, by category:		
	Reported internally	**Reported to US-CERT**	**Reported to law enforcement**
Type of Incident:	**Number of Incidents**	**Number of Incidents**	**Number of Incidents**
a. Unauthorized Access			
b. Denial of Service (DoS)			
c. Malicious Code	47,680	24	0
d. Improper Usage			
e. Other	1	1	
Totals:	47681	25	0

Comments:

Internal malicious code incidents include all adware, marketware, etc. The incidents marked critical were reported to US-CERT. Other represents an incident involving Personally Identifiable Information. Data was collected from October 2005 to August 2006.

Section B: Questions 6 and 7
Nuclear Regulatory Commission (NRC)
Date: 9/14/2006

Question 6

6. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities? Yes or No.	Yes

a. Total number of employees	b. Number of employees that received IT security awareness training during the past fiscal year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003)		c. Total number of employees with significant IT security responsibilities	d. Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998)		e. Total costs for providing IT security training in the past fiscal year (in $'s)
	Number	Percentage		Number	Percentage	
3712	3670	99%	115	80	70%	$315,000

6.f. Briefly describe the training provided in b. and d:

Comments:

During the fiscal year, new staff were provided initial IT security awareness training, all staff were provided refresher IT security 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 awareness training. The on-line awareness course includes the following topics: Threats-Vulnerabilities, Malicious Software, Passwords, Internet Security, Mobile Computing, Personal Use, Software Licenses, Marking (of media), Reporting Incidents, and (User) Responsibilities. The course ends with a ten-question quiz as well as the opportunity for employees to answer three bonus questions before printing out their certificate of completion. The Information Systems Security Officers Awareness Course includes the following topics: Planning and Budgeting, Policy and Regulations, Risk Management, Personnel Security, Security Controls, Continuity of Operations, Certification, and Procurement, as well as a quiz and certificate.

IT training includes: IT security related seminars, meetings, conferences, university courses, and vendor specific related courses.

Question 7

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

Section B: Chief Information Officer. Question 8, 9, and 10.
Nuclear Regulatory Commission (NRC)
Date: 9/14/2006

Question 8

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

8.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	N/A	No	
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	N/A	No	
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. AIX, Sybase, Novell	Yes	Yes	- Almost Always, or on approximately 96-100% of the systems running this software
Comments:			

Question 9

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.

9.a.	The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.	Yes
9.b.	The agency follows documented policies and procedures for external reporting to law enforcement authorities. Yes or No.	Yes
9.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 10		
10.a.	Has the agency documented in its security policies special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)? Yes or No.	Yes
10.b.	If the answer to 10 a. is “Yes,” briefly describe the documented procedures. These special procedures could include more frequent control tests & evaluations, specific configuration requirements, additional monitoring, or specialized training.	
The NRC has a draft wireless policy, "Requirements for Using Wireless Technologies for Broadband Remote Desktop," and will be developing policies for IPv6 and other emerging technologies as needed.		
Comments:		