

Section B - Chief Information Officer: Questions 1 and 2

Agency Name: Nuclear Regulatory Commission **Submission date:** October 1, 2008

Question 1: FISMA Systems Inventory

1. In the table below, identify the number of agency and contractor information systems by component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized). Extend the worksheet onto subsequent pages if necessary to include all Component/Bureaus.

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.

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.

Question 2: Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

2. For the Total Number of Systems identified by Component/Bureau and FIPS System Impact Level in the table for Question 1, identify the number and percentage of systems which have: a current certification and accreditation, security controls tested and reviewed within the past year, and a contingency plan tested within in accordance with policy.

Bureau Name	FIPS 199 System Impact Level	Question 1			Question 2					
		a. Agency Systems	b. Contractor Systems	c. Total Number of Systems (Agency and Contractor systems)	a. Number of systems certified and accredited		b. Number of systems for which security controls have been tested and reviewed in the past year		c. Number of systems for which contingency plans have been tested in accordance with policy	
		Number	Number	Total Number	Total Number	Percent of Total	Total Number	Percent of Total	Total Number	Percent of Total
Nuclear Reg Comm	High	11	1	12	5	42%	12	100%	12	100%
	Moderate	17	9	26	17	65%	25	96%	26	100%
	Low		1	1	1	100%	1	100%	1	100%
	Not Categorized			0						
	Sub-total	28	11	39	23	59%	38	97%	39	100%
N/A	High			0						
	Moderate			0						
	Low			0						
	Not Categorized			0						
	Sub-total	0	0	0	0		0		0	
N/A	High			0						
	Moderate			0						
	Low			0						
	Not Categorized			0						
	Sub-total	0	0	0	0		0		0	
N/A	High			0						
	Moderate			0						
	Low			0						
	Not Categorized			0						
	Sub-total	0	0	0	0		0		0	
N/A	High			0						
	Moderate			0						
	Low			0						
	Not Categorized			0						
	Sub-total	0	0	0	0		0		0	
N/A	High			0						
	Moderate			0						
	Low			0						
	Not Categorized			0						
	Sub-total	0	0	0	0		0		0	
Agency Totals	High	11	1	12	5	42%	12	100%	12	100%
	Moderate	17	9	26	17	65%	25	96%	26	100%
	Low	0	1	1	1	100%	1	100%	1	100%
	Not Categorized	0	0	0	0		0		0	
	Total	28	11	39	23	59%	38	97%	39	100%

= Data Entry Cells
 = Editable Calculations (no Data Entry-ONLY edit Formulas when necessary)

Section B - Chief Information Officer: Questions 3 and 4

Agency Name: Nuclear Regulatory Commission

Question 3: Implementation of Security Controls in NIST Special Publication 800-53

3a. Has the organization developed policies and corresponding procedures to cover all NIST SP 800-53 control families, and associated 800-53 security controls? Yes or No.	Yes
---	-----

3.b. Please describe your annual testing and continuous monitoring process: NRC requires annual System Security Plan updates or revalidation plus contingency plan updating and test results annually. NRC performs Annual Security Control Testing of all major applications and general support systems. NRC requires quarterly Plan of Action and Milestone updates from all system owners and periodically performs penetration testing and vulnerability scanning on selected systems and on all systems undergoing security testing/evaluation.	
---	--

Question 4: Incident Detection, Monitoring, and Response Capabilities

What tools, techniques, technologies, etc., does the agency use for incident detection?

4.a. NRC uses Dragon and Snort as network Intrusion Detection Systems (IDS) on critical network segments. Multiple layers of Antivirus - on servers, desktops, e-mail application servers, and the e-mail gateways. All web traffic is scanned for malicious scripting behavior, viruses, trojans and other malware. Host-based system integrity software (Tripwire) is utilized on critical servers. NRC maintains and monitors firewall, proxy server, e-mail, and web content filtering device logs. Log entries are compared with malicious host lists provided by US CERT and other Agencies.	
---	--

4.b. How many systems (or networks of systems) are protected using the tools, techniques and technologies described in 4 (a) above?	31
--	----

4.c. Does the agency log and monitor activities involving access to and modification of sensitive or critical information? Yes or No.	Yes
--	-----

4.d. What percentage of systems maintain audit trails that provide a trace of user actions?	94.00%
--	--------

4.e. Does the agency maintain an incident handling and response capability? Yes or No.	Yes
---	-----

4.f. If the answer to 4 (e) is yes, what percentage of systems are operated within the agency's incident handling and response capability?	100.00%
---	---------

What tools, techniques, technologies, etc. does the agency use for incident handling and response?

4.g. NRC has a dedicated Computer Security Incident Response Team (CSIRT) with 24/7 coverage. The CSIRT uses NRC policies and procedures and US CERT guidelines to identify, triage, investigate, remediate and recover from all computer security incidents. NRC is a GFIRST member and works closely with and provides reports on reportable incidents to US CERT within the US CERT prescribed timeframes. NRC maintains an Incident Report Listing and has detailed reports on each incident.	
--	--

Section B - Chief Information Officer: Questions 5 and 6

Agency Name: Nuclear Regulatory Commission

Question 5: Security Awareness Training

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

Yes

5.b. Report the following for your agency:

b.1.	b.2.		b.3.	b.4.	b.5.		b.6.
Total number of employees (including contractors)	Number of employees and contractors that received information 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)		Number of employees and contractors that received information security awareness training using an ISSLOB shared service center. (breakout of total for b)	Total number of employees with significant information security responsibilities	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)		Total costs for providing information security training in the past fiscal year (in \$'s)
	Number	Percentage	Number		Number	Percentage	
4540	4378	96%	0%	550	60	11%	\$ 100,931

5.c. Briefly describe the training provided in 5.b.2. and 5.b.5 and how you measure its effectiveness.

Computer security awareness was provided using a web based training on iLearn with a test at the completion. Users were required to obtain a 70% or higher test score to successfully complete the training. Those with significant security responsibilities in the area of system owner, system administrator, and ISSOs also received training. System owner and system administrator training was in-person training and the ISSO course was web based.

Question 6: Peer-to-Peer file sharing

Does the agency explain policies regarding the use of collaborative web technologies and peer-to-peer file sharing in information security awareness training, ethics training, or any other agency-wide training? Yes or No.

Yes

Section B - Chief Information Officer: Questions 7

Question 7: Configuration Management

7.a.	Is there an agency wide security configuration policy? Yes or No.	Yes
7.b.	<p>Approximate the extent to which applicable systems implement common security configurations including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov.</p> <p>Response categories:</p> <ul style="list-style-type: none"> - 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 (81-95% of the time)
7.c.	Indicate which aspects of Federal Desktop Core Configuration (FDCC) have been implemented as of this report:	
	c.1. Agency has adopted and implemented FDCC standard configurations and has documented deviations. Yes or No.	Yes
	c.2 New Federal Acquisition Regulation 2007-004 language, which modified "Part 39—Acquisition of Information Technology", is included in all contracts related to common security settings. Yes or No.	Yes
	c.3 All Windows XP and VISTA computing systems have implemented the FDCC security settings. Yes or No.	No

Section B - Chief Information Officer: Questions 8, 9, and 10

Agency Name:

Nuclear Regulatory Commission

Question 8: Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.

- | | | |
|-------------|---|-----|
| 8.a. | The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No. | Yes |
| 8.b. | The agency follows documented policies and procedures for external reporting to US-CERT. Yes or No. (http://www.us-cert.gov) | Yes |
| 8.c. | The agency follows documented policies and procedures for reporting to law enforcement. Yes or No. | Yes |

Comments:

Question 9: New Technologies and Emerging Threats

- | | | |
|-------------|---|-----|
| 9.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 |
|-------------|---|-----|

- 9.b.** If the answer to 9a. 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.

Emerging technologies must be certified and accredited and their use approved by the Designated Approving Authorities (DAA). NRC has issued policies limiting the use of wireless implementations except within specific implementations approved by the DAAs. NRC is following the OMB mandate on IPv6 and completed testing to ensure the backbone is IPv6 compatible. Logical access to NRC systems and sensitive information will be incorporated into the HSPD-12 identity cards by October 2011. NRC uses IDSs, Firewalls, DMZ, and Antivirus tools.

Question 10: Performance Metrics for Security Policies and Procedures

Please provide three (3) outcome/output-based performance metrics your agency uses to measure the effectiveness or efficiency of security policies and procedures. The metrics must be different than the ones used in these FISMA reporting instructions, and can be tailored from NIST's Special Publication 800-55 "Performance Measurement Guide for Information Security."

Performance Metric Name	Description
System Security Plans (SSP) Updated	How many systems have their SSP updated annually
Personally Identifiable Information (PII) breaches	How many PII breaches occur annually at NRC
Plan of Action and Milestones (POA&M)	How many POA&M weaknesses are opened/closed each quarter

YN Yes
No AgencyName

YNNA Yes
No
NA

Quarters FY07 Q4
FY08 Q1
FY08 Q2
FY08 Q3
FY08 Q4
FY09 Q1
FY09 Q2
FY09 Q3
FY09 Q4
FY10 Q1
FY10 Q2
FY10 Q3
FY10 Q4

FIPS-IMPACTLEVEL
High
Moderate
Low
Not Categorized
Sub-total

X_Marker X

Department of Agriculture
Department of Commerce
Department of Defense
Department of Education
Department of Energy
Department of Health and Human Services
Department of Homeland Security
Department of Housing and Urban Development
Department of Interior
Department of Justice
Department of Labor
Department of State
Agency for International Development (USAID)
Department of Transportation
Department of Treasury
Department of Veterans Affairs
Corps of Engineers
Environmental Protection Agency
General Services Administration
National Aeronautics and Space Administration
National Archives and Records Administration
National Science Foundation
Nuclear Regulatory Commission
Executive Office of the President
Office of Personnel Management
Small Business Administration
Smithsonian Institution
Social Security Administration
Legislative Branch
Judicial Branch
Federal Drug Control Programs
International Assistance Programs (not including USAID)
Other Civil Defense Programs
Advisory Council on Historic Preservation
Appalachian Regional Commission
Architectural and Transportation Barriers Compliance Board
Barry Goldwater Scholarship and Excellence in Education Foundation
Central Intelligence Agency
Commission of Fine Arts
Commission on Civil Rights
Committee for Purchase from People who are Blind or Severely Disabled
Commodity Futures Trading Commission
Consumer Product Safety Commission
Corporation for Public Broadcasting
U.S. Court of Appeals for Veterans Claims
Defense Nuclear Facilities Safety Board
District of Columbia (Courts...)
Equal Employment Opportunity Commission
Export-Import Bank of the US
Farm Credit Administration
Farm Credit System Financial Assistance Corporation
Farm Credit System Insurance Corporation

Federal Communications Commission
Federal Deposit Insurance Corporation
Federal Election Commission
Federal Financial Institutions Examination Council Appraisal Subcommittee
Federal Housing Finance Board
Federal Labor Relations Authority
Federal Maritime Commission
Federal Mediation and Conciliation Service
Federal Mine Safety and Health Review Commission
Federal Retirement Thrift Investment Board
Federal Trade Commission
Harry S. Truman Scholarship Foundation
Institute of American Indian and Alaska Native Culture and Arts Development
U.S. Interagency Council on Homelessness
International Trade Commission
James Madison Memorial Fellowship Foundation
Japan-United State Friendship Commission
Legal Services Corporation
Marine Mammal Commission
Merit Systems Protection Board
National Capital Planning Commission
National Commission on Libraries and Information Science
National Council on Disability
National Credit Union Administration
National Endowment for the Arts
National Endowment for the Humanities
National Labor Relations Board
National Mediation Board
National Transportation Safety Board
Neighborhood Reinvestment Corporation
Nuclear Waste Technical Review Board
Occupational Safety and Health Review Commission
Office of Government Ethics
Office of Navajo and Hopi Indian Relocation
Office of Special Counsel
Panama Canal Commission
Postal Service
Railroad Retirement Board
Resolution Trust Corporation
Securities and Exchange Commission
State Justice Institute
Tennessee Valley Authority
U.S. Holocaust Memorial Museum
U.S. Institute of Peace
Christopher Columbus Fellowship Foundation
Intelligence Community Management Account
Institute of Museum and Library Services
United Mine Workers of America Benefit Funds
Corporation for National and Community Service
U.S. Enrichment Corporation Fund
Morris K. Udall Scholarship and Excellence in National Environmental Policy Foundation
National Education Goals Panel

Other Commissions and Boards
Community Empowerment Board
Chemical Safety and Hazard Investigation Board
Court Services and Offender Supervision Agency for the District of Columbia
Presidio Trust
Denali Commission
Broadcasting Board of Governors
Commission on Ocean Policy
Oklahoma City National Memorial Trust
Delta Regional Authority
National Veterans Business Development Corporation
Vietnam Education Foundation
White House Commission on the National Moment of Remembrance
U.S. Canada Alaska Rail Commission
Pacific Chapter Commission
Election Assistance Commission
SEC Public Accounting Oversight Board
SEC Standard Setting Body
Telecommunications Development Fund
Affordable Housing Program
Electric Reliability Organization
Federal Housing Enterprise Regulator
Affordable Housing and Bank Enterprise
Federal Law Enforcement Training Center
JFK Assassination Records Review Board
FarmCredit System
Federal Home Loan Bank System
Federal Home Loan Mortgage Corporation
Federal National Mortgage Association
Student Loan Marketing Association
Financing Vehicles and the Board of Governors of the Federal Reserve
Selective Service System
Arlington National Cemetery
Millennium Challenge Corporation
Inter-American Foundation
Peace Corps
U.S. Trade and Development Agency
Overseas Private Investment Corporation
National Gallery of Art

BureauName Administration for Children and Families
Administration of Foreign Affairs
Administration on Aging
Administrative Office of the United States
African Development Foundation
Agency for Healthcare Research and Quality
Agency for International Development
Agricultural Marketing Service
Agricultural Research Service
Alcohol and Tobacco Tax and Trade Bureau
Allowances
American Battle Monuments Commission
Animal and Plant Health Inspection Service
Architect of the Capitol
Armed Forces Retirement Home
Bank Insurance
Benefits Programs
Botanic Garden
Bureau of Alcohol, Tobacco, Firearms, and Explosives
Bureau of Engraving and Printing
Bureau of Indian Affairs
Bureau of Industry and Security
Bureau of Labor Statistics
Bureau of Land Management
Bureau of Mines
Bureau of Reclamation
Bureau of the Census
Bureau of the Public Debt
Capitol Police
Cemeterial Expenses
Centers for Disease Control and Prevention
Centers for Medicare and Medicaid Services
Central Utah Project
Citizenship and Immigration Services
Community Planning and Development
Comptroller of the Currency
Construction
Cooperative State Research, Education, and Extension Service
Courts of Appeals, District Courts, and other Judicial Services
Department of Defense Agencies
Department of the Air Force
Department of the Army
Department of the Navy
Departmental Administration
Departmental Management
Departmental Offices
Deposit Insurance
District of Columbia Courts
District of Columbia General and Special Payments
Domestic Nuclear Detection Office
Drug Enforcement Administration
Economic and Statistical Analysis

Economic Development Administration
Economic Development Challenge
Economic Research Service
Educational Benefits
Employee Benefits Security Administration
Employment and Training Administration
Employment Standards Administration
Energy Programs
Environmental and Other Defense Activities
Executive Operations
Fair Housing and Equal Opportunity
Family Housing
Farm Service Agency
FDIC-Office of Inspector General
Federal Aviation Administration
Federal Bureau of Investigation
Federal Emergency Management Agency
Federal Financing Bank
Federal Highway Administration
Federal Motor Carrier Safety Administration
Federal Prison System
Federal Railroad Administration
Federal Student Aid
Federal Transit Administration
Financial Crimes Enforcement Network
Financial Management Service
Food and Drug Administration
Food and Nutrition Service
Food Safety and Inspection Service
Foreign Agricultural Service
Forest and Wildlife Conservation, Military Reservations
Forest Service
FSLIC Resolution
General Activities
General Administration
Government Accountability Office
Government National Mortgage Association
Government Printing Office
Grain Inspection, Packers and Stockyards Administration
Health Resources and Services Administration
House of Representatives
Housing Programs
Hurricane Education Recovery
Indian Health Services
Information Analysis and Infrastructure Protection
Institute of Education Sciences
Insular Affairs
Interagency Law Enforcement
Interagency Law Enforcement
Inter-American Foundation
Interest on the Public Debt
Internal Revenue Service

International Commissions
International Monetary Programs
International Organizations and Conferences
International Reconstruction and Other Assistance
International Security Assistance
International Trade Administration
Joint Items
Judicial Retirement Funds
Legal Activities and US Marshals
Library of Congress
Management and Administration
Maritime Administration
Military Construction
Military Personnel
Military Retirement
Military Sales Program
Millennium Challenge Corporation
Mine Safety and Health Administration
Minerals Management Service
Minority Business Development Agency
Multilateral Assistance
National Agricultural Statistics Service
National Highway Traffic Safety Administration
National Indian Gaming Commission
National Institute of Standards and Technology
National Institutes of Health
National Nuclear Security Administration
National Oceanic and Atmospheric Administration
National Park Service
National Security Division
National Technical Information Service
National Telecommunications and Information Administration
Natural Resources Conservation Service
Natural Resources Damage Assessment and Restoration
Occupational Safety and Health Administration
Office of Civil Rights
Office of Communications
Office of Compliance
Office of Elementary and Secondary Education
Office of English Language Acquisition
Office of Housing Finance Oversight
Office of Indian Education
Office of Innovation and Improvement
Office of Justice Programs
Office of Lead Hazard Control and Healthy Homes
Office of Postsecondary Education
Office of Safe and Drug-Free Schools
Office of Special Education and Rehabilitative Services
Office of Special Trustee for American Indians
Office of Surface Mining Reclamation and Enforcement
Office of the General Counsel
Office of the Inspector General

Office of the Secretary
Office of the Solicitor
Office of Thrift Supervision
Office of Vocational and Adult Education
Operation and Maintenance
Overseas Private Investment Corporation
Peace Corps
Pension Benefit Guaranty Corporation
Pipeline and Hazardous Materials Safety Administration
Policy Development and Research
Power Marketing Administration
Preparedness
Procurement
Program Support Center
Public and Indian Housing Programs
Radiation Exposure Compensation
Real Property Activities
Research and Innovative Technology Administration
Research, Development, Test, and Evaluation
Retiree Health Care
Revolving and Management Funds
Risk Management Agency
Rural Business—Cooperative Service
Rural Development
Rural Housing Service
Rural Utilities Service
Saint Lawrence Seaway Development Corporation
Savings Association Insurance
Science and Technology
Security, Enforcement, and Investigations
Selective Service System
Senate
Special Assistance Initiatives
Special Foreign Currency Program
Substance Abuse and Mental Health Services Administration
Supply and Technology Activities
Supreme Court of the United States
Surface Transportation Board
Technology Administration
Trade and Development Agency
Trust Funds
U.S. Patent and Trademark Office
United States Coast Guard
United States Court of Appeals for the Federal Circuit
United States Court of International Trade
United States Fish and Wildlife Service
United States Geological Survey
United States Mint
United States Parole Commission
United States Secret Service
United States Sentencing Commission
United States Tax Court

Veterans Health Administration
Violent Crime Reduction Trust Fund