Group D

FOIA/PA NO: 2014-0217

RECORDS BEING RELEASED IN PART

The following types of information are being withheld:

Ex. 1: ☐ Records properly classified pursuant to Executive Order 13526
Ex. 2: ☐ Records regarding personnel rules and/or human capital administration
Ex. 3: ☐ Information about the design, manufacture, or utilization of nuclear weapons
☐ Information about the protection or security of reactors and nuclear materials
☐ Contractor proposals not incorporated into a final contract with the NRC
☐ Other_____
Ex. 4: ☐ Proprietary information provided by a submitter to the NRC
☐ Other_____
Ex. 5: ☑ Draft documents or other pre-decisional deliberative documents (D.P. Privilege)
☐ Records prepared by counsel in anticipation of litigation (A.W.P. Privilege)
☐ Privileged communications between counsel and a client (A.C. Privilege)
☐ Other_____
Ex. 6: ☐ Agency employee PII, including SSN, contact information, birthdates, etc.
☐ Third party PII, including names, phone numbers, or other personal information
Ex. 7(A): ☐ Copies of ongoing investigation case files, exhibits, notes, ROI's, etc.
☐ Records that reference or are related to a separate ongoing investigation(s)
Ex. 7(C): ☐ Special Agent or other law enforcement PII
☐ PII of third parties referenced in records compiled for law enforcement purposes
Ex. 7(D): ☐ Witnesses' and Allegers' PII in law enforcement records
☐ Confidential Informant or law enforcement information provided by other entity
Ex. 7(E): ☐ Law Enforcement Technique/Procedure used for criminal investigations
☐ Technique or procedure used for security or prevention of criminal activity
Ex. 7(F): ☑ Information that could aid a terrorist or compromise security

Other/Comments:_____
_____

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

April 11, 2014

The Honorable Fred Upton
Chairman, Committee on Energy
and Commerce
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On behalf of the Commission, and based on a request for additional detail, I am transmitting an addendum to the February 2014 monthly status report on the U.S. Nuclear Regulatory Commission (NRC) activities and utilization of unobligated carryover funds appropriated from the Nuclear Waste Fund. As you are aware, the report describes the NRC actions that were taken in February 2014 to address the remand by the U.S. Court of Appeals for the District of Columbia Circuit in In re Aiken County, regarding the licensing process for the Department of Energy's Yucca Mountain license application.

The addendum is marked "FOR OFFICIAL USE ONLY – SENSITIVE INTERNAL INFORMATION" and in the way of a reminder, we respectfully ask that these handling instructions be honored.

Please feel free to contact me at (301) 415-1776 if you have questions or need more information.

Sincerely,

V. Renee Simpson
Director, Office of Congressional Affairs

Enclosure:
As stated

cc: Representative Henry A. Waxman

D/1

Identical letter sent to:

The Honorable Fred Upton
Chairman, Committee on Energy
and Commerce
United States House of Representatives
Washington, DC 20515
cc: Representative Henry A. Waxman

The Honorable John Shimkus
Chairman, Subcommittee on Environment
and the Economy
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515
cc: Representative Paul Tonko

The Honorable Barbara Boxer
Chairman, Committee on Environment
and Public Works
United States Senate
Washington, DC 20510
cc: Senator David Vitter

The Honorable Sheldon Whitehouse
Chairman, Subcommittee on Clean Air
and Nuclear Safety
Committee on Environment
and Public Works
United States Senate
Washington, DC 20510
cc: Senator Jeff Sessions

The Honorable Ed Whitfield
Chairman, Subcommittee on Energy
and Power
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515
cc: Representative Bobby L. Rush

The Honorable Harold Rogers
Chairman, Committee on Appropriations
United States House of Representatives
Washington, DC 20515
cc: Representative Nita Lowey

The Honorable Mike Simpson
Chairman, Subcommittee on Energy
and Water Development
Committee on Appropriations
United States House of Representatives
Washington, DC 20515
cc: Representative Marcy Kaptur

The Honorable Dianne Feinstein
Chairman, Subcommittee on Energy
and Water Development
Committee on Appropriations
United States Senate
Washington, DC 20510
cc: Senator Lamar Alexander

(b)(5),(b)(7)(F)

(b)(5)

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

February 8, 2013

The Honorable Fred Upton
Chairman, Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am providing the enclosed copy of the Fiscal Year 2012 Federal Information Security Management Act (FISMA) Report, including the required transmittal letter to the Office of Management and Budget.

The NRC is fully committed to maintaining the security of its automated information systems. Please contact me if you have any questions regarding the NRC FISMA report.

Sincerely,

Rebecca L. Schmidt, Director
Office of Congressional Affairs

Enclosure:
NRC FY12 FISMA Report

cc: Representative Henry A. Waxman

D12

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

CHAIRMAN

November 14, 2012

Mr. Jeffrey D. Zients
Deputy Director for Management
The Office of Management and Budget
725 17th Street, NW
Washington, DC 20503

Dear Mr. Zients:

On behalf of the U.S. Nuclear Regulatory Commission (NRC), I am providing the Fiscal Year (FY) 2012 Federal Information Security Management Act (FISMA) Report. The enclosed FY 2012 NRC FISMA and Privacy Management Reports consist of the following four documents:

- NRC Chief Information Officer Section Report
- NRC Senior Agency Official for Privacy Section Report
- NRC Progress Update on Actions Taken to Protect Personally Identifiable Information/Social Security Numbers
- NRC Inspector General Section Report

Since submitting last year's report, the NRC continues to function at a high level of assurance of information security and continues to make progress in FISMA compliance and with the agency's privacy management program. In the past year, the NRC completed security assessments and authorizations of four new systems, reauthorized four systems, split the Information Technology Infrastructure into two systems, and retired one system. In an effort to further improve its authorization activities, the NRC also consolidated five existing systems into three existing systems. The current reportable systems at the NRC stand at 23.

In the upcoming year, the NRC anticipates continued progress in FISMA compliance through increased continuous monitoring and an improved risk management program. We will continue to update your staff on the NRC's progress in accordance with OMB and Department of Homeland Security instructions. If you have any questions about the FY 2012 NRC FISMA and Privacy Management Reports, please contact me or have your staff contact Mr. Darren B. Ash, Deputy Executive Director for Corporate Management, at (301) 415-7443.

Sincerely,

Allison M. Macfarlane

Enclosures:
As stated

Chief Information Officer

Section Report

2012

Annual FISMA Report

Nuclear Regulatory Commission

Section 1: System Inventory

1.1 For each of the FIPS 199 systems categorized impact levels (H = High, M = Moderate, L = Low) in this question, provide the total number of Organization information systems by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below. (Organizations with below 5000 users may report as one unit.)

1.2 For each of the FIPS 199 system categorized impact levels in this question, provide the total number of Organization operational, information systems using cloud services by Organization component (i.e. Bureau or Sub-Department Operating Element) in the table below.

Agency/ Component	1.1a Organization Operated Systems	1.1b Contractor Operated Systems	1.1c Systems (from 1.1a and 1.1b) with Security ATO	1.2a Systems utilizing cloud computing resources	1.2b Systems utilizing cloud computing resources (1.2a) with a Security Assessment and Authorization	1.2c Systems in 1.2a utilizing a FedRAMP authorized Cloud Service Provider
NRC			(b)(7)(F)			
Agency Totals						

Section 2: Asset Management

2.0 **Hardware Assets: Provide the total number of organization hardware assets connected to the organization's unclassified network(s).**

(b)(7)(F)

2.1 **Provide the number of assets in 2.0, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.**

(b)(7)(F)

2.1a **How often are these automated capabilities (device discovery processes) conducted on all assets connected to the organization's full network(s)? (frequency in days)**

(b)(7)(F)

2.1a(1) **How much time does it take a device discovery tool to complete this process? (Duration in days; e.g. 10 days or 0.2 days)**

(b)(7)(F)

2.1b **Provide the number of assets in 2.0, where all of the following information is collected: Network IP address, Machine Name, MAC Address (or other hardware identifier like serial number).**

(b)(7)(F)

2.2 **Provide the number of assets in 2.0, where the organization has an automated capability to determine whether the asset is authorized and to determine who manages it.**

(b)(7)(F)

2.3 **Provide the number of assets in 2.0, where the organization has an automated capability to compare 2.1 and 2.2, to identify and remove (manually or through NAC, etc.) the unauthorized devices.**

(b)(7)(F)

Comments: (b)(7)(F)

2.3a **For the assets in 2.3, how much time does it actually take to a) assign for management (authorize) or b) remove unauthorized devices once discovered with 95% confidence? (Duration in days; e.g. 10.00 days or 0.20 days)**

(b)(7)(F)

Comments: (b)(7)(F)

Section 2: Asset Management

2.3b **Provide the number of assets in 2.0, where the Organization has implemented an automated capability to detect and mitigate unauthorized routes, including routes across air-gapped networks.**

(b)(7)(F)

Comments: (b)(7)(F)

2.4 **Software Assets: Can the organization track the installed operating system Vendor, Product, Version, and patch-level combination(s) in use on the assets in 2.0?**

(b)(7)(F)

2.4.a **Can the organization track, (for each installed operating system Vendor, Product, Version, and patch-level combination in 2.4) the number of assets in 2.1 on which it is installed in order to assess the number of operating system vulnerabilities which are present without scanning?**

(b)(7)(F)

2.5 **Does the Organization have a current list of the enterprise-wide COTS general purpose applications (e.g., Internet Explorer, Adobe, Java, MS Office, Oracle, SQL, etc.) installed on the assets in 2.0?**

(b)(7)(F)

2.5a **For each enterprise-wide COTS general purpose applications in 2.5, can the Organization report the number of assets in 2.0 on which it is installed by CPE in order to know the number of application vulnerabilities which are present without scanning?**

Yes

2.6 **Provide the number of assets in 2.0, where the Organization has implemented an automated capability to detect and block unauthorized software from executing, or where no such software exists for the device type.**

(b)(7)(F)

Comments: (b)(7)(F)

Section 3: Configuration Management

3.1 **For each operating system Vendor, Product, Version, and patch-level combination referenced in 2.4, report the following:**

Section 3: Configuration Management

3.1a Whether an adequately secure configuration baseline has been defined.

(b)(7)(F)

Comments: (b)(7)(F)

3.1b The number of hardware assets with this software (which are covered by this baseline, if it exists).

(b)(7)(F)

3.1c For what percentage of the applicable hardware assets (per question 2.0), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1a and provide visibility at the organization's enterprise level?

(b)(7)(F)

3.1d How frequently is the identification of deviations conducted? (Answer in days, per General Instructions)

(b)(7)(F)

Comments: (b)(7)(F)

3.2 For each of the enterprise-wide COTS general purpose applications Vendor, Product, Version, and patch-level combination referenced in question 2.5., report:

3.2a Whether an adequately secure configuration baseline has been defined.

(b)(7)(F)

Comments: (b)(7)(F)

3.2b The number of hardware assets with this software (which are covered by this baseline, if it exists).

(b)(7)(F)

3.2c For what percentage of the applicable hardware assets, with each kind of software in 3.2, has an automated capability to identify configuration deviations from the approved defined baselines and provide visibility at the organization's enterprise level?

(b)(7)(F)

Section 3: Configuration Management

3.2d How frequently is the identification of deviations conducted? (Answer in days, per General Instructions)

(b)(7)(F)

Comments: (b)(7)(F)

3.3 Report the number of hardware assets from 2.0 to which the FDCC/USGCB baseline applies.

(b)(7)(F)

3.3a Report the number of CCEs in the FDCC/USGCB baselines where the organization has approved deviations from the FDCC/USGCB standard across the organization (or organizational sub-components). List those specific CCEs in the comment.

(b)(7)(F)

Comments: (b)(7)(F)

3.3b For each CCE in 3.3a, indicate in the comment the CCE and the number of assets in 2.1 to which the FDCC/USGCB standard applies, but has been relaxed (through an approved deviation) by the organization. Report the sum of these numbers (count of asset-CCE pairs that have been relaxed) in the response.

(b)(7)(F)

Section 4: Vulnerability and Weakness Management

4.1 Provide the number of hardware assets identified in section 2.0 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.

(b)(7)(F)

4.1.1 Provide the number of hardware assets identified in section 2.0 that were evaluated using tools to assess the security of the systems and that generated output compliant with each of the following:

4.1.1a Common Vulnerabilities and Exposures (CVE)

(b)(7)(F)

4.1.1b Common Vulnerability Scoring System (CVSS)

(b)(7)(F)

Section 4: Vulnerability and Weakness Management

4.1.1c Open Vulnerability and Assessment Language (OVAL)

(b)(7)(F)

4.2 National Vulnerability Database (NVD) and the Secure Content Automation Program (SCAP) are focused primarily on common COTS operating systems and applications, after they are released. However, COTS and non-COTS software need to be searched for weaknesses before release. It is often useful to check open–source software for weaknesses, if the developer has not thoroughly done so. What methods has your organization considered using to find, identify and assess weaknesses that may be in software that your organization develops and uses?

a. Identify Universe Enumeration	a. Have you considered using this tool?	b. Are you using this now?	c. Describe this method	d. Is this a viable solution?	What are the obsticles?
Common Weakness Enumeration (CWE)	(b)(7)(F)				
Web scanners for web-based applications					
Common Attack Pattern Enumeration and Classification					
b. Find Instances Tools and Languages					
Static Code Analysis Tools	(b)(7)(F)				
Manual code reviews (especially for weaknesses not covered by the automated tools)					
Dynamic Code Analysis Tools					
Web scanners for web-based applications					
PEN testing for attack types not covered by the automated tools.					
c. Assess Importance					
Common Weakness Scoring System (CWSS)	(b)(7)(F)				

Section 4: Vulnerability and Weakness Management

4.2d **List any other viable methods your organization has considered using to find, identify, and assess weaknesses that may be in software that your organization develops and uses?**

Method Type	Tool Name	a. Have you considered using this method?	b. Are you using this now?	c. Describe this method	d. What are the Obstacles?
(b)(7)(F)					

4.3 **For what percentage of information systems does the organization:**

Impact Level	For systems in development and/or maintenance: Use methods described in section 4.2 to identify and fix instances of common weaknesses, prior to placing that version of the code into production?	For systems in development and/or maintenance: Can you find SCAP compliant tools and good SCAP content?	For systems in production: Report on configuration and vulnerability levels for hardware assets supporting those systems, giving application owners an assessment of risk inherited from the general support system (network)?	For systems in production: Can you find SCAP compliant tools and good SCAP content?
High	(b)(7)(F)			
Moderate				
Low				

Section 5: Identity and Access Management

5.1 **What is the number of Organization unprivileged network user accounts? (Exclude privileged network user accounts and non-user accounts)**

(b)(7)(F)

Section 5: Identity and Access Management

5.2 How many unprivileged network user accounts are configured to:

Comments: (b)(7)(F)

	Require the form of identification listed on the left?		Allow, but not require, the form of identification listed on the left?	
a. User-ID and Password		(b)(7)(F)		(b)(7)(F)
b. Two factor-PIV Card				
c. Other two factor authentication				

5.3 What is the number of Organization privileged network user accounts? (Exclude non-user accounts and unprivileged network user accounts)

(b)(7)(F)

Comments: (b)(7)(F)

5.4 How many privileged network user accounts are configured to:

Comments: (b)(7)(F)

	Require the form of identification listed on the left?		Allow, but not require, the form of identification listed on the left?	
a. User-ID and Password		(b)(7)(F)		(b)(7)(F)
b. Two factor-PIV Card				
c. Other two factor authentication				

5.5 What is the number of Organization unprivileged (high and moderate impact) application user accounts? (Exclude privileged application user accounts and non-user accounts)

N/A

Comments: (b)(7)(F)

Section 5: Identity and Access Management

5.6 How many unprivileged application user accounts are configured to:

Comments: (b)(7)(F)

	Require the form of identification listed on the left?		Allow, but not require, the form of identification listed on the left?	
a. User-ID and Password		(b)(7)(F)		(b)(7)(F)
b. Two factor-PIV Card				
c. Other two factor authentication				

5.7 What is the number of Organization privileged application user accounts? (Exclude non-user accounts and unprivileged application user accounts)

(b)(7)(F)

Comments: (b)(7)(F)

5.8 How many privileged application user accounts are configured to:

Comments: (b)(7)(F)

	Require the form of identification listed on the left?		Allow, but not require, the form of identification listed on the left?	
a. User-ID and Password		(b)(7)(F)		(b)(7)(F)
b. Two factor-PIV Card				
c. Other two factor authentication				

5.9 Provide the percent of privileged network users whose privileges were reviewed this year for:

5.9a Privileges on that account reconciled with work requirements

(b)(7)(F)

5.9b Adequate separation of duties considering aggregated privileges on all accounts for the same person (user)

(b)(7)(F)

5.9c Provide the percent of privileged network users whose privileges were adjusted or terminated after being reviewed this year.

(b)(7)(F)

Section 5: Identity and Access Management

5.10 **Describe any best practices your Organization has developed in any of the following areas which are generally difficult in Federal Organizations.**

5.10a **Methods to identify accounts that actually have elevated privileges even though not intended or indicated by the account name.**

(b)(7)(F)

Comments: (b)(7)(F)

5.10b **Methods used to accurately and automatically identify all of the accounts assigned to the same person.**

(b)(7)(F)

5.10c **Methods used to identify all account holders who have departed location or service and should have their accounts disabled and removed, especially if your method covers all account holders (your organization's direct hire employees, institutional contractors, persons detailed to your organization from others, locally engaged staff overseas, etc.) by the same method.**

(b)(7)(F)

Section 6: Data Protection

6.1 **Provide the estimated number of hardware assets from Question 2.0 which have the following characteristics. Enter responses in the table.**

Mobile Assets Types (each asset should be recorded no more than once in each column)	Estimated number of mobile hardware assets of the types indicated in each row		Estimated number assets from column a with adequate encryption of data on the device.	
Laptop Computers, Netbooks and Tablet-Type Computers		(b)(7)(F)		(b)(7)(F)
Personal Digital Assistant				
BlackBerries and Other Smartphones				
USB connected devices (e.g., Flashdrives and Removable Hard Drives)				
Other mobile hardware assets (describe types in comments field)				

Section 6: Data Protection

6.2 **Provide the percentage of Organization email traffic on systems that implement FIPS 140-2 compliant encryption technologies to protect the integrity of the contents and sender information when sending messages to government agencies or the public, such as S/MIME, PGP, OpenPGP, or PKI.**

(b)(7)(F)

Comments: (b)(7)(F)

6.3 **Select the description that best describes your Organization's PKI Certificate Authority, and respond with the number of that option.**

(b)(7)(F)

6.4 **What percentage of the applicable Security Controls from NIST SP 800-53A (profiled by FPKIPA) does the PKI Certificate Authority and related PKI Infrastructure your organization uses adequately satisfy?**

(b)(7)(F)

Section 7: Boundary Protection

7.1 **Provide the percentage of the required TIC 1.0 Capabilities that are implemented.**

(b)(7)(F)

7.1a **Provide the percentage of TIC 2.0 Capabilities that are implemented.**

(b)(7)(F)

7.2 **Provide the percentage of TICs with operational NCPS (Einstein) deployment.**

(b)(7)(F)

7.2a **Provide the percentage of TICs with operational Einstein 2 deployment.**

(b)(7)(F)

7.2b **Provide the percentage of TICs with operational Einstein 3 deployment.**

(b)(7)(F)

Section 7: Boundary Protection

7.3 Provide the percentage of external network traffic to/from the organization's networks passing through a TIC/MTIPS.

(b)(7)(F)

7.4 Provide the percentage of external network/application interconnections to/from the organization's networks passing through a TIC/MTIPS.

(b)(7)(F)

7.5 Provide the percentage of Organization email systems that implement sender verification (anti-spoofing) technologies when sending messages.

(b)(7)(F)

7.6 Provide the percentage of Organization email systems that check sender verification (anti-spoofing) technologies to detect possibly forged messages from outside the network.

(b)(7)(F)

7.7 Provide the estimated percent of incoming email traffic (measured in messages) where the link/attachment is executed/opened in a sandbox/virtual environment in-line to ascertain whether or not it is malicious, and quarantined as appropriate, before it can be opened by the recipient. (Note: If you consider this to be infeasible, please explain why in the comments.)

(b)(7)(F)

7.8 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization conducts scheduled scans for unauthorized wireless access points (WAP) connected to an Organizational network.

(b)(7)(F)

Comments: (b)(7)(F)

(b)(7)(F) Provide the percentage of hardware assets, identified in section 2.0 (Asset Management), which are in facilities where WAP scans are conducted.

(b)(7)(F)

7.9 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization conducts unscheduled scans for unauthorized wireless access points.

(b)(7)(F)

Comments: (b)(7)(F)

Section 7: Boundary Protection

7.10 Provide the frequency (in days, e.g., 30.0 or 0.25) in which the Organization maps their cyber perimeter (e.g. publically accessible systems, externally visible systems and devices) for each network.

(b)(7)(F)

7.11 Provide the percent of client browsers that are required to run only in a virtual environment.

(b)(7)(F)

7.12 What percentage of network boundary devices are assessed by an automated capability to ensure that they continue to be adequately free of vulnerabilities and are adequately configured as intended, such as to adequately protect security?

(b)(7)(F)

7.13 Provide the number of cloud systems from question 1.2a where traffic entering and exiting the cloud:

7.13a does not pass through a TIC?

(b)(7)(F)

7.13b are not required to pass through a TIC?

(b)(7)(F)

7.14 Provide the number of networks with DLP/DRM at the gateway to capture outbound data leakage (e.g., PII).

(b)(7)(F)

Section 8: Incident Management

8.1 What is the number of Organization hardware assets (from question 2.0) on networks on which controlled network penetration testing was performed in the reporting period?

(b)(7)(F)

Comments: (b)(7)(F)

8.1a Percentage of applicable events detected by NOC/SOC during the penetration test.

(b)(7)(F)

Comments: (b)(7)(F)

Section 8: Incident Management

8.1b Median time to detection of applicable events. (Time in days and fractions of days. See General Instructions.)

(b)(7)(F)

Comments: (b)(7)(F)

8.2 During FY12, for what percentage of US-CERT Security Awareness Reports (SARs), or the equivalent for DoD, has the organization adequately remediated or acted upon the actionable recommendations contained in the report? Please use the Comment function to comment on how the SAR process is meeting its goal and/or could be improved.

(b)(7)(F)

Comments: (b)(7)(F)

8.3 Provide the percentage of incidents that have been detected and attributed to successful phishing attacks. Please provide a Comment to describe any innovative and effective ways your organization has found to address these attacks.

(b)(7)(F)

Comments: (b)(7)(F)

Section 9: Training and Education

9.1 Provide the number of the Organization's network users that have been given and successfully completed cybersecurity awareness training in FY2012 (at least annually).

(b)(7)(F)

Comments: (b)(7)(F)

9.1a Provide the estimated percentage of new users to satisfactorily complete security awareness training before being granted network access, or within an organizationally defined time limit, providing adequate security, after being granted access.

(b)(7)(F)

Comments: (b)(7)(F)

Section 9: Training and Education

9.2 To what extent were users given cybersecurity awareness training content more frequently than annually (content could include a single question or tip of the day)?

Comments: (b)(7)(F)

Bureau	Frequency with which users receive supplemental cybersecurity awareness training
NRC	Daily

9.2a Provide the average frequency in days between content provision. See General Instructions.

(b)(7)(F)

Comments: (b)(7)(F)

9.2b Provide the percentage of this additional content that addresses emerging threats that were not previously covered in the annual training?

(b)(7)(F)

9.2c At what frequency is security awareness training content (that is provided to users) updated by the Organization or training provider? (Average frequency in days during FY2012. See General Instructions.)

(b)(7)(F)

Comments: (b)(7)(F)

9.2d Provide the total number of Organization-sponsored emerging threat exercises (such as phishing) designed to increase cybersecurity awareness and/or to measure the effectiveness of cybersecurity awareness training in molding behavior.

(b)(7)(F)

Comments: (b)(7)(F)

9.2e Provide the percentage of exercises in 9.2d where either no problems were found, or in which the problems were addressed through appropriate training within three months.

(b)(7)(F)

Comments: (b)(7)(F)

Section 9: Training and Education

9.3 Provide the number of the Organization's network users and other staff with significant security responsibilities.

(b)(7)(F)

9.3a Provide the number of people in 9.3 that have been given training to perform their significant cybersecurity responsibilities at an organizationally defined frequency that has been determined to provide adequate security.

(b)(7)(F)

9.3b Provide the longest organizationally defined frequency that has been determined to provide adequate security for any role among those included in significant security responsibilities. (Days between training events. See general instructions)

(b)(7)(F)

Comments: (b)(7)(F)

9.3c At what frequency is training to perform their significant cybersecurity responsibilities updated by the Organization or training provider? (Average frequency in days across roles during FY2012. See General Instructions.)

(b)(7)(F)

Comments: (b)(7)(F)

Section 10: Remote Access

10.1 Provide the estimated total number of annual remote connections the Organization provides to allow users to connect to near-full access to the Organization's normal desktop LAN/WAN resources/services.

(b)(7)(F)

Comments: (b)(7)(F)

10.1a For those connections counted above in 10.1, provide the estimated number of those connections that:

For each type of connection listed below, please provide the number of connections that use the authentication method listed to the right. Type of Connection	ONLY User-ID and Password	ONLY Two factor-PIV	ONLY Other two factor authentication	Only one other (please describe in the comments)	Connections that may have been authenticated multiple ways
Dial-Up	(b)(7)(F)	(b)(7)(F)	(b)(7)(F)	(b)(7)(F)	(b)(7)(F)
Virtual Private Network (not clientless)					
Virtual Private Network (clientless) including SSL, TLS, etc.					
Citrix					
Other					

Section 10: Remote Access

10.1b For those connections counted above in 10.1a column e), provide the estimated number of those connections that:

For each type of connection listed below, please provide the number of connections that use the authentication method listed to the right. Type of Connection	User-ID and Password	Two factor-PIV Card	Other two factor authentication	Other(s). (Please describe in the comments.)
Dial-Up	(b)(7)(F)	(b)(7)(F)	(b)(7)(F)	(b)(7)(F)
Virtual Private Network (not clientless)				
Virtual Private Network (clientless) including SSL, TLS, etc.				
Citrix				
Other				

10.1c For those connections counted above in 10.1, provide the estimated percentage of those connections that:

Comments: (b)(7)(F)

Utilize FIPS 140-2 validated cryptographic modules.

(b)(7)(F)

Prohibit split tunneling and/or dual-connected remote hosts where the laptop has two active connections.

(b)(7)(F)

Are configured in accordance with OMB M-07-16, to time-out after 30 minutes of inactivity (or less) requiring re-authentication to reestablish session.

(b)(7)(F)

Scan for malware upon connection.

(b)(7)(F)

Require Government Furnished Equipment (GFE).

(b)(7)(F)

Section 10: Remote Access

Assess and correct system configuration upon connection of GFE.

(b)(7)(F)

Section 11: Network Security Protocols

11.1 Provide the number of public facing domain names (second-level, e.g. www.dhs.gov). (You should exclude domain names which host only FIPS 199 low-impact information on ISPs.)

(b)(7)(F)

11.1a Provide the number of DNS names from 11.1, signed using DNSSEC.

(b)(7)(F)

11.1b Provide the percentage of the second-level DNS names from 11.1 and their sub-domains for which all domain names at and under the second level are signed.

(b)(7)(F)

11.2 Provide the percentage of public facing servers that use IPv6 (e.g., web servers, email servers, DNS servers, etc.). (Exclude low-impact networks, cloud servers, and ISP resources from the numerator and denominator unless they require IPv6 to perform their business function.)

(b)(7)(F)

Comments: (b)(7)(F)

Inspector General

Section Report

2012

Annual FISMA Report

Nuclear Regulatory Commission

Section 1: Continuous Monitoring Management

1.1 Has the Organization established an enterprise-wide continuous monitoring program that assesses the security state of information systems that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

1.1.1 Documented policies and procedures for continuous monitoring (NIST 800-53: CA-7)

Yes

1.1.2 Documented strategy and plans for continuous monitoring (NIST 800-37 Rev 1, Appendix G)

Yes

1.1.3 Ongoing assessments of security controls (system-specific, hybrid, and common) that have been performed based on the approved continuous monitoring plans (NIST 800-53, NIST 800-53A)

Yes

1.1.4 Provides authorizing officials and other key system officials with security status reports covering updates to security plans and security assessment reports, as well as POA&M additions and updates with the frequency defined in the strategy and/or plans (NIST 800-53, NIST 800-53A)

Yes

1.2 Please provide any additional information on the effectiveness of the Organization's Continuous Monitoring Management Program that was not noted in the questions above

None

Section 2: Configuration Management

2.1 Has the Organization established a security configuration management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

2.1.1 Documented policies and procedures for configuration management

Yes

Section 2: Configuration Management

2.1.2 Standard baseline configurations defined

Yes

Comments: The FY 2011 FISMA independent evaluation found that baseline configurations were not implemented on some NRC systems. Vulnerability scanning performed as part of ST&E (conducted in support of the security assessment and authorization process) and annual security control testing identified numerous vulnerabilities that demonstrate non-compliance with required baseline configurations in several systems. As a result, the OIG issued two recommendations to address this finding. They are being tracked on the agency's POA&M and have a target completion date of December 30, 2013.

2.1.3 Assessing for compliance with baseline configurations

Yes

Comments: The FY 2011 FISMA independent evaluation found that software compliance assessment procedures are not consistently implemented. For example, for one system that has been operational for many years, there was no evidence any vulnerability scans had been done on that system. For another system that has also been operational for many years, scans conducted during the ST&E found numerous vulnerabilities. As a result, the OIG issued two recommendations to address this finding. They are being tracked on the agency's POA&M and have a target completion date of June 30, 2014.

2.1.4 Process for timely, as specified in Organization policy or standards, remediation of scan result deviations

Yes

Comments: The FY 2011 FISMA independent evaluation found that vulnerabilities are not always remediated in a timely manner. Some systems that have been operational for many years were found with a number of vulnerabilities found during pervious scans that had not been remediated within the timeframes required by the agency. As a result, the OIG issued one recommendation to address this finding. It is being tracked on the agency's POA&M and has a target completion date of June 30, 2014.

2.1.5 For Windows-based components, FDCC/USGCB secure configuration settings fully implemented and any deviations from FDCC/USGCB baseline settings fully documented

Yes

2.1.6 Documented proposed or actual changes to hardware and software configurations

Yes

2.1.7 Process for timely and secure installation of software patches

Yes

Section 2: Configuration Management

2.1.8 **Software assessing (scanning) capabilities are fully implemented (NIST 800-53: RA-5, SI-2)**

Yes

2.1.9 **Configuration-related vulnerabilities, including scan findings, have been remediated in a timely manner, as specified in Organization policy or standards. (NIST 800-53: CM-4, CM-6, RA-5, SI-2)**

Yes

2.1.10 **Patch management process is fully developed, as specified in Organization policy or standards. (NIST 800-53: CM-3, SI-2)**

Yes

2.2 **Please provide any additional information on the effectiveness of the Organization's Configuration Management Program that was not noted in the questions above.**

See additional narrative

Comments:	NRC has remote locations housing IT system components from multiple NRC systems, including infrastructure and a badging system, as well as NRC-managed systems that support the remote location. One of the remote locations also houses IT system components supporting the NRC Continuity of Operations Plan and IT system components that provide disaster recovery support for some NRC systems and another remote location also houses IT system components that provide disaster recovery support for some NRC systems.During site visits to three NRC remote locations, the OIG found that while information system component inventories exist for individual NRC systems, there are no up-to-date consolidated inventories for the components of these systems located in the remote locations, associated rack diagrams are not up-to-date, and the inventories do not meet NRC requirements. See the Independent Evaluation of NRC's Implementation of FISMA for FY 2012 report, Finding #2, for additional details.

Section 3: Identity and Access Management

3.1 **Has the Organization established an identity and access management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and identifies users and network devices? Besides the improvement opportunities that have been identified by the OIG, does the program include the following attributes:**

Yes

3.1.1 **Documented policies and procedures for account and identity management (NIST 800-53: AC-1)**

Yes

3.1.2 **Identifies all users, including federal employees, contractors, and others who access Organization systems (NIST 800-53, AC-2)**

Yes

Section 3: Identity and Access Management

3.1.3 Identifies when special access requirements (e.g., multi-factor authentication) are necessary.

Yes

3.1.4 If multi-factor authentication is in use, it is linked to the Organization's PIV program where appropriate (NIST 800-53, IA-2)

Yes

3.1.5 Organization has adequately planned for implementation of PIV for logical access in accordance with government policies (HSPD 12, FIPS 201, OMB M-05-24, OMB M-07-06, OMB M-08-01, OMB M-11-11)

Yes

3.1.6 Ensures that the users are granted access based on needs and separation of duties principles

Yes

3.1.7 Identifies devices with IP addresses that are attached to the network and distinguishes these devices from users (For example: IP phones, faxes, printers are examples of devices attached to the network that are distinguishable from desktops, laptops or servers that have user accounts)

Yes

3.1.8 Identifies all User and Non-User Accounts (refers to user accounts that are on a system. Examples of non-user accounts are accounts such as an IP that is set up for printing. Data user accounts are created to pull generic information from a database or a guest/anonymous account for generic login purposes that are not associated with a single user or a specific group of users)

Yes

3.1.9 Ensures that accounts are terminated or deactivated once access is no longer required

Yes

3.1.10 Identifies and controls use of shared accounts

Yes

3.2 Please provide any additional information on the effectiveness of the Organization's Identity and Access Management Program that was not noted in the questions above.

None

Section 4: Incident Response and Reporting

Section 4: Incident Response and Reporting

4.1 Has the Organization established an incident response and reporting program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

4.1.1 Documented policies and procedures for detecting, responding to and reporting incidents (NIST 800-53: IR-1)

Yes

4.1.2 Comprehensive analysis, validation and documentation of incidents

Yes

4.1.3 When applicable, reports to US-CERT within established timeframes (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.4 When applicable, reports to law enforcement within established timeframes (SP 800-86)

Yes

4.1.5 Responds to and resolves incidents in a timely manner, as specified in Organization policy or standards, to minimize further damage. (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.1.6 Is capable of tracking and managing risks in a virtual/cloud environment, if applicable

Yes

4.1.7 Is capable of correlating incidents

Yes

4.1.8 There is sufficient incident monitoring and detection coverage in accordance with government policies (NIST 800-53, 800-61, and OMB M-07-16, M-06-19)

Yes

4.2 Please provide any additional information on the effectiveness of the Organization's Incident Management Program that was not noted in the questions above.

None

Section 5: Risk Management

Section 5: Risk Management

5.1 **Has the Organization established a risk management program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

5.1.1 **Documented and centrally accessible policies and procedures for risk management, including descriptions of the roles and responsibilities of participants in this process**

Yes

5.1.2 **Addresses risk from an organization perspective with the development of a comprehensive governance structure and organization-wide risk management strategy as described in NIST 800-37, Rev.1**

Yes

Comments: The FY 2011 FISMA independent evaluation found that the agency has not developed or implemented an organization-wide risk management strategy in accordance with government policies. As a result, the OIG issued a recommendation to address this finding. It is being tracked on the agency's POA&M and has a target completion date of December 30, 2013.

5.1.3 **Addresses risk from a mission and business process perspective and is guided by the risk decisions at the organizational perspective, as described in NIST 800-37, Rev.1**

Yes

5.1.4 **Addresses risk from an information system perspective and is guided by the risk decisions at the organizational perspective and the mission and business perspective, as described in NIST 800-37, Rev. 1**

Yes

5.1.5 **Categorizes information systems in accordance with government policies**

Yes

Comments: In response to recommendations from previous independent evaluations, the agency developed an automated inventory system and developed procedures, guides, and user manuals that provide guidance for maintaining system inventory records within that system. These procedures, guides and user manuals describe the system inventory process, the basic requirements for entering new system inventory data into the agency's automated inventory system, the methodology for entering data into security records within that system, and instructions on working with system inventory and security program information in that system. The agency also provides inventory instructions with its biannual inventory update data call. However, despite all of these instructions, the OIG found that the NRC system inventory is not up-to-date. See the Independent Evaluation of NRC's Implementation of FISMA for FY 2012 report, Finding #1, for additional details.

Section 5: Risk Management

5.1.6 Selects an appropriately tailored set of baseline security controls

Yes

5.1.7 Implements the tailored set of baseline security controls and describes how the controls are employed within the information system and its environment of operation

Yes

5.1.8 Assesses the security controls using appropriate assessment procedures to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system

Yes

5.1.9 Authorizes information system operation based on a determination of the risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation of the information system and the decision that this risk is acceptable

Yes

5.1.10 Ensures information security controls are monitored on an ongoing basis including assessing control effectiveness, documenting changes to the system or its environment of operation, conducting security impact analyses of the associated changes, and reporting the security state of the system to designated organizational officials

Yes

5.1.11 Information system specific risks (tactical), mission/business specific risks and organizational level (strategic) risks are communicated to appropriate levels of the organization.

Yes

5.1.12 Senior Officials are briefed on threat activity on a regular basis by appropriate personnel. (e.g., CISO).

Yes

5.1.13 Prescribes the active involvement of information system owners and common control providers, chief information officers, senior information security officers, authorizing officials, and other roles as applicable in the ongoing management of information system-related security risks

Yes

5.1.14 Security authorization package contains system security plan, security assessment report, and POA&M in accordance with government policies. (SP 800-18, SP 800-37)

Yes

Section 5: Risk Management

5.1.15 Security authorization package contains Accreditation boundaries for Organization information systems defined in accordance with government policies.

Yes

5.2 Please provide any additional information on the effectiveness of the Organization's Risk Management Program that was not noted in the questions above.

None

Section 6: Security Training

6.1 Has the Organization established a security training program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

6.1.1 Documented policies and procedures for security awareness training (NIST 800-53: AT-1)

Yes

6.1.2 Documented policies and procedures for specialized training for users with significant information security responsibilities

Yes

6.1.3 Security training content based on the organization and roles, as specified in Organization policy or standards

Yes

6.1.4 Identification and tracking of the status of security awareness training for all personnel (including employees, contractors, and other Organization users) with access privileges that require security awareness training

Yes

6.1.5 Identification and tracking of the status of specialized training for all personnel (including employees, contractors, and other Organization users) with significant information security responsibilities that require specialized training

Yes

6.1.6 Training material for security awareness training contains appropriate content for the Organization (SP 800-50, SP 800-53).

Yes

Section 6: Security Training

6.2 **Please provide any additional information on the effectiveness of the Organization's Security Training Program that was not noted in the questions above.**

None

Section 7: Plan Of Action & Milestones (POA&M)

7.1 **Has the Organization established a POA&M program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracks and monitors known information security weaknesses? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

7.1.1 **Documented policies and procedures for managing IT security weaknesses discovered during security control assessments and requiring remediation**

Yes

Comments:

NRC has developed a formal POA&M process that describes the process for identifying, assessing, prioritizing, and monitoring the progress of corrective actions pertaining to security weaknesses and provides agency direction for the management and tracking of corrective efforts relative to known weaknesses in IT security controls. However, the OIG found that the agency's POA&M process is not consistently followed. As a result, the agency's POA&Ms are not effective at monitoring the progress of corrective efforts relative to known weaknesses in IT security controls. Specifically, POA&Ms do not include all known security weaknesses (see 7.1.6), POA&Ms are not updated in a timely manner (see 7.1.8), scheduled completion dates are being changed (see 7.1.4), and risk management activities are not added to the POA&M as required (see 7.1.2). See the Independent Evaluation of NRC's Implementation of FISMA for FY 2012 report, Finding #3, for additional details.

7.1.2 **Tracks, prioritizes and remediates weaknesses**

Yes

Comments:

Each year, the agency issues an annual IT security risk management activities memorandum. Instructions included with this memorandum require system owners to add annual contingency plan testing, annual security control testing, and security-related document updates, including annual system security plan update to their system's POA&Ms. However, the OIG found that these activities were not added to POA&Ms for 7 of the agency's 22 systems.

7.1.3 **Ensures remediation plans are effective for correcting weaknesses**

Yes

Section 7: Plan Of Action & Milestones (POA&M)

7.1.4 Establishes and adheres to milestone remediation dates

Yes

Comments: The agency's POA&M process states that once the scheduled completion date is set, it should not be changed. However, the OIG found multiple instances of changed scheduled completion dates. As a result, weakness are being reported as on track when in fact they are actually delayed resulting in inaccurate reporting to OMB.

7.1.5 Ensures resources are provided for correcting weaknesses

Yes

7.1.6 POA&Ms include security weaknesses discovered during assessments of security controls and requiring remediation. (Do not need to include security weakness due to a Risk Based Decision to not implement a security control) (OMB M-04-25)

Yes

Comments: The agency's POA&M process requires POA&Ms to be updated to add vulnerabilities identified as part of an independent assessment such as security testing and evaluation, continuous monitoring, vulnerability assessment report, security assessment report, security impact assessment. U.S. Government Accountability Office report, or OIG report. These weaknesses must be added to the POA&M as soon as possible, but not to exceed 60 days from the assessor's report. However, the OIG found some IT-related weaknesses were not added to the POA&M as required by agency policy.

7.1.7 Costs associated with remediating weaknesses are identified (NIST SP 800-53, Rev. 3, Control PM-3 and OMB M-04-25)

Yes

7.1.8 Program officials and contractors report progress on remediation to CIO on a regular basis, at least quarterly, and the CIO centrally tracks, maintains, and independently reviews/validates the POA&M activities at least quarterly (NIST SP 800-53, Rev. 3, Control CA-5, and OMB M-04-25)

Yes

Comments: The agency's POA&M process requires POA&Ms to be updated within the agency's automated tool by the system owner with the most current information by the 15th of November, February, May, and August. However, the OIG found POA&Ms are not updated in a timely manner.

Section 7: Plan Of Action & Milestones (POA&M)

7.2 **Please provide any additional information on the effectiveness of the Organization's POA&M Program that was not noted in the questions above.**

See additional narrative

Comments: The agency implemented a tool for automating the POA&M process that was put into place to ensure the agency's POA&M procedures are implemented consistently, completely, and accurately. However, the OIG found that the agency's POA&M tool does not implement key OMB and NRC POA&M requirements. As a result, the NRC's POA&M process is not consistently implemented. Specifically, the tool allows scheduled completion dates to be changed, allows weaknesses to be created without a scheduled completion date, allows weaknesses to be created with no value in the field that identifies the source of the weakness, allows weaknesses to be closed without specifying an actual completion date, and does not automatically change the status from on track to delayed once the scheduled completion date has passed. It also allows users to enter actual completion dates in the future. See the Independent Evaluation of NRC's Implementation of FISMA for FY 2012 report, Finding #4, for additional details.

Section 8: Remote Access Management

8.1 **Has the Organization established a remote access program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:**

Yes

8.1.1 **Documented policies and procedures for authorizing, monitoring, and controlling all methods of remote access (NIST 800-53: AC-1, AC-17)**

Yes

8.1.2 **Protects against unauthorized connections or subversion of authorized connections.**

Yes

8.1.3 **Users are uniquely identified and authenticated for all access (NIST 800-46, Section 4.2, Section 5.1)**

Yes

8.1.4 **Telecommuting policy is fully developed (NIST 800-46, Section 5.1)**

Yes

8.1.5 **If applicable, multi-factor authentication is required for remote access (NIST 800-46, Section 2.2, Section 3.3)**

Yes

Section 8: Remote Access Management

8.1.6 Authentication mechanisms meet NIST Special Publication 800-63 guidance on remote electronic authentication, including strength mechanisms

Yes

8.1.7 Defines and implements encryption requirements for information transmitted across public networks

Yes

8.1.8 Remote access sessions, in accordance to OMB M-07-16, are timed-out after 30 minutes of inactivity after which re-authentication are required

Yes

8.1.9 Lost or stolen devices are disabled and appropriately reported (NIST 800-46, Section 4.3, US-CERT Incident Reporting Guidelines)

Yes

8.1.10 Remote access rules of behavior are adequate in accordance with government policies (NIST 800-53, PL-4)

Yes

8.1.11 Remote access user agreements are adequate in accordance with government policies (NIST 800-46, Section 5.1, NIST 800-53, PS-6)

Yes

8.2 Please provide any additional information on the effectiveness of the Organization's Remote Access Management that was not noted in the questions above.

None

Section 9: Contingency Planning

9.1 Has the Organization established an enterprise-wide business continuity/disaster recovery program that is consistent with FISMA requirements, OMB policy, and applicable NIST guidelines? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

9.1.1 Documented business continuity and disaster recovery policy providing the authority and guidance necessary to reduce the impact of a disruptive event or disaster (NIST 800-53: CP-1)

Yes

Section 9: Contingency Planning

9.1.2 **The Organization has performed an overall Business Impact Analysis (BIA) (NIST SP 800-34)**

Yes

9.1.3 ***Development and documentation of division, component, and IT infrastructure recovery strategies, plans and procedures* (NIST SP 800-34)**

Yes

Comments: NRC has developed several types of plans that support FISMA and NIST requirements to develop plans and procedures to ensure continuity of operations for information systems that support agency operations and assets. For example, NRC has developed a continuity of operations plan (COOP) and information system contingency plans for all systems in the agency's inventory of systems. However, the OIG found that contingency planning for the agency's IT environment needs improvement. Specifically, the IT environment contingency plan does not address contingency events that don't require relocation to an alternate site, and procedures specific to contingency planning for NRC remote locations are not up-to-date. In addition, the COOPs for NRC remote locations are not current and only address situations where IT environment components at headquarters are not available. See the Independent Evaluation of NRC's Implementation of FISMA for FY 2012 report, Finding #5, for additional details.

9.1.4 **Testing of system specific contingency plans**

Yes

9.1.5 **The documented business continuity and disaster recovery plans are in place and can be implemented when necessary (FCD1, NIST SP 800-34)**

Yes

9.1.6 **Development and fully implementable of test, training, and exercise (TT&E) programs (FCD1, NIST SP 800-34, NIST 800-53)**

Yes

9.1.7 **Performance of regular ongoing testing or exercising of business continuity/disaster recovery plans to determine effectiveness and to maintain current plans**

Yes

9.1.8 **After-action report that addresses issues identified during contingency/disaster recovery exercises (FCD1, NIST SP 800-34)**

Yes

9.1.9 **Systems that have alternate processing sites (FCD1, NIST SP 800-34, NIST SP 800-53)**

Yes

Section 9: Contingency Planning

9.1.10 **Alternate processing sites are subject to the same risks as primary sites (FCD1, NIST SP 800-34, NIST SP 800-53)**

No

Comments: Alternate processing sites for those NRC systems that require them are sufficiently distant from the primary processing site so they are not subject to the same risks as the primary sites. The majority of alternate processing sites ar over 1000 miles from the primary sites. There are two alternate processing sites between 140 and 240 miles from the primary sites, so they could potentially be subject to the same risk as the primary site, but only in extreme circumstances.

9.1.11 **Backups of information that are performed in a timely manner (FCD1, NIST SP 800-34, NIST SP 800-53)**

Yes

9.1.12 **Contingency planning that consider supply chain threats**

Yes

9.2 **Please provide any additional information on the effectiveness of the Organization's Contingency Planning Program that was not noted in the questions above.**

None

Section 10: Contractor Systems

10.1 **Has the Organization established a program to oversee systems operated on its behalf by contractors or other entities, including Organization systems and services residing in the cloud external to the Organization? Besides the improvement opportunities that may have been identified by the OIG, does the program includes the following attributes:**

Yes

10.1.1 **Documented policies and procedures for information security oversight of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud**

Yes

10.1.2 **The Organization obtains sufficient assurance that security controls of such systems and services are effectively implemented and comply with federal and Organization guidelines**

Yes

10.1.3 **A complete inventory of systems operated on the Organization's behalf by contractors or other entities, including Organization systems and services residing in public cloud**

Yes

Section 10: Contractor Systems

10.1.4 The inventory identifies interfaces between these systems and Organization-operated systems (NIST 800-53: PM-5)

Yes

10.1.5 The Organization requires appropriate agreements (e.g., MOUs, Interconnection Security Agreements, contracts, etc.) for interfaces between these systems and those that it owns and operates

Yes

10.1.6 The inventory of contractor systems is updated at least annually.

Yes

10.1.7 Systems that are owned or operated by contractors or entities, including Organization systems and services residing in public cloud, are compliant with FISMA requirements, OMB policy, and applicable NIST guidelines

Yes

10.2 Please provide any additional information on the effectiveness of the Organization's Contractor Systems Program that was not noted in the questions above.

None

Section 11: Security Capital Planning

11.1 Has the Organization established a security capital planning and investment program for information security? Besides the improvement opportunities that may have been identified by the OIG, does the program include the following attributes:

Yes

11.1.1 Documented policies and procedures to address information security in the capital planning and investment control (CPIC) process

Yes

11.1.2 Includes information security requirements as part of the capital planning and investment process

Yes

11.1.3 Establishes a discrete line item for information security in organizational programming and documentation (NIST 800-53: SA-2)

Yes

11.1.4 Employs a business case/Exhibit 300/Exhibit 53 to record the information security resources required (NIST 800-53: PM-3)

Yes

Section 11: Security Capital Planning

11.1.5 Ensures that information security resources are available for expenditure as planned

Yes

11.2 Please provide any additional information on the effectiveness of the Organization's Security Capital Planning Program that was not noted in the questions above.

None

Senior Agency Official For Privacy

Section Report

2012
Annual
FISMA

Nuclear Regulatory Commission

Question 1: Information Security Systems

		1a. Number of Federal systems that contain personal information in an identifiable form			1b. Number of systems in column a. for which a Privacy Impact Assessment (PIA) is required under the E-Government Act			1c. Number of systems in column b. covered by a current PIA				1d. Number of systems in column a. for which a System of Records Notice (SORN) is required under the Privacy Act			1e. Number of systems in column d. for which a current SORN has been published in the Federal Register			
Agency/ Component	Submission Ststus	Agency Owned Systems	Contractor Owned Systems	Total Systems	Agency Owned Systems	Contractor Owned Systems	Total Systems	Agency Owned Systems	Contractor Owned Systems	Total Systems	% Complete	Agency Owned Systems	Contractor Owned Systems	Total Systems	Agency Owned Systems	Contractor Owned Systems	Total Systems	% Complete
NRC	Submitted to Agency	34	12	46	16	7	23	16	7	23	100%	24	9	33	24	9	33	100%
Agency Totals		34	12	46	16	7	23	16	7	23	100%	24	9	33	24	9	33	100%

Section 2: PIAs and SORNs

2a **Provide the URL of the centrally located page on the agency web site that provides working links to agency PIAs (N/A if not applicable).**

http://www.nrc.gov/site-help/plans/privacy-impcat-asess.html

2b **Provide the URL of the centrally located page on the agency web site that provides working links to the published SORNs (N/A if not applicable)**

http://www.nrc.gov/reading-rm/foia/privacy-systems.html

Section 3: Senior Agency Official for Privacy (SAOP) Responsibilities

3a **Can your agency demonstrate with documentation that the SAOP participates in all agency information privacy compliance activities?**

Yes

3b **Can your agency demonstrate with documentation that the SAOP participates in evaluating the privacy implications of legislative, regulatory, and other policy proposals, as well as testimony and comments under OMB Circular A-19?**

No

3c **Can your agency demonstrate with documentation that the SAOP participates in assessing the impact of the agencys use of technology on privacy and the protection of personal information?**

Yes

Section 4: Privacy Training

Section 4: Privacy Training

4a **Does your agency have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations, and policies, and understand the ramifications of inappropriate access and disclosure?**

Yes

Comments: In response to Office of Management and Budget (OMB) recommendation in memorandum (M-07-16), the NRC issued the Management Directive 3.2 which describe the NRC privacy policy. Additionally, All NRC employees and contractors must take the "Personally Identifiable Information (PII) Responsibilities Awareness and Acknowledgement of Understanding" course annually.

4b **Does your agency have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) that handle personal information, that are directly involved in the administration of personal information or information technology systems, or that have significant information security responsibilities?**

Yes

Section 5: PIA and Web Privacy Policies and Processes

5 **Does the agency have a written policy or process for each of the following?**

5a **PIA Practices**

5a(1) **Determining whether a PIA is needed.**

Yes

Comments: The Privacy Impact Assessment (PIA) guidance is posted on the NRC Internal Web server.

5a(2) **Conducting a PIA.**

Yes

Comments: The Privacy Impact Assessment (PIA) manual is posted on the NRC Internal Web server.

5a(3) **Evaluating changes in technology or business practices that are identified during the PIA process.**

Yes

Comments: The PIA process is included in the Project Management Methodology (PMM) and in the system authorization process.

5a(4) **Ensuring systems owners, privacy officials, and IT experts participate in conducting the PIA.**

Yes

Comments: The PIA process is included in the Project Management Methodology and it is required as part of the system security categorization.

Section 5: PIA and Web Privacy Policies and Processes

5a(5) **Making PIAs available to the public as required by law and OMB policy.**

Yes

5a(6) **Monitoring the agencys systems and practices to determine when and how PIAs should be updated.**

Yes

5a(7) **Assessing the quality and thoroughness of each PIA and performing reviews to ensure that appropriate standards for PIAs are maintained.**

Yes

5b **Web Privacy Practices**

5b(1) **Determining circumstances where the agencys web-based activities warrant additional consideration of privacy implications.**

Yes

Comments: Management Directive 3.14 address the U.S. Nuclear Regulatory Commission Public Web Site.

5b(2) **Making appropriate updates and ensuring continued compliance with stated web privacy policies.**

Yes

5b(3) **Requiring machine-readability of public-facing agency web sites (i.e., use of P3P).**

Yes

Section 6: Conduct of Mandated Reviews

Component / Bureau	a. Section (m) Contracts	b. Records Practices	c. Routine Uses	d. Exemp-tions	e. Matching Programs	f. Training	g. Violations: Civil Action	h. Violations: Remedial Action	i. System of Records Notices	j. (e)(3) Statement	k. Privacy Impact Assessments and Updates	l. Data Mining Impact Assessment
NRC	N	N	Y	0	0	Y	N	N	39	12	11	N
	Records Practices - reviewed by RASS every 2 years. Routine Uses - completed on 9/12 a total of 39 reviews completed during the biennial system of records reviews with each of the system managers. Training is done once a year, last completed in FY 2012. System of Records Notice FY12 all 39 systems reviewed. Statements - 12 agency formes reviewed. PIA and Updates FY12 - 11 reviews completed.											
TOTAL				***0***	***0***				***39***	***12***	11	

Section 7: Written Privacy Complaints

7 **Indicate the number of written complaints for each type of privacy issue received by the SAOP or others at the agency.**

Section 7: Written Privacy Complaints

7a Process and Procedural — consent, collection and appropriate notice.

0

7b Redress — non-Privacy Act inquiries seeking resolution of difficulties or concerns about privacy matters.

0

7c Operational — inquiries regarding Privacy Act matters not including Privacy Act requests for access and/or correction.

0

7d Referrals — complaints referred to another agency with jurisdiction.

0

Section 8: Policy Compliance Review

8a Does the agency have current documentation demonstrating review of the agency's compliance with information privacy laws, regulations, and policies?

Yes

8b Can the agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews?

Yes

8c Does the agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices?

Yes

8d Does the agency coordinate with the agency's Inspector General on privacy program oversight?

Yes

Section 9: SAOP Advice and Guidance

9 Please select "Yes" or "No" to indicate if the SAOP has provided formal written advice or guidance in each of the listed categories, and briefly describe the advice or guidance if applicable.

9a Agency policies, orders, directives or guidance governing the agency's handling of personally identifiable information.

Yes

9b Written agreements (either interagency or with non-Federal entities) pertaining to information sharing, computer matching and similar issues.

No

Section 9: SAOP Advice and Guidance

9c The agency's practices for conducting, preparing and releasing SORNs and PIAs.

Yes

9d Reviews or feedback outside of the SORN and PIA process (e.g., formal written advice in the context of budgetary or programmatic activities or planning).

No

9e Privacy training (either stand-alone or included with training on related issues).

Yes

Section 10: Agency Use of Web Management and Customization Technologies (e.g., "cookies," "tracking technologies")

10a Does the agency use web management and customization technologies on any web site or application?

No

10b Does the agency annually review the use of web management and customization technologies to ensure compliance with all laws, regulations and OMB guidance?

No

10c Can the agency demonstrate, with documentation, the continued justification for, and approval to use, web management and customization technologies?

No

10d Can the agency provide the notice language or citation for the web privacy policy that informs visitors about the use of web management and customization technologies?

No

Progress Update on Actions Taken to Protect Personally Identifiable Information/Social Security Numbers

October 5, 2012

U.S. Nuclear Regulatory Commission

Progress Update on Actions Taken to Protect Personally Identifiable Information/Social Security Number

The U.S. Nuclear Regulatory Commission (NRC) has completed all actions identified in its "Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers," dated September 19, 2007. To build on the efforts identified in this plan, the NRC continues to develop and issue policy and procedures to protect personally identifiable information (PII), which includes the Social Security number (SSN), and to eliminate or reduce its unnecessary collection and use. Below are the actions that have been taken by the NRC to protect PII.

1. Agency Policy Issued on Safeguarding Personally Identifiable Information

The NRC has developed policies and procedures to implement guidance from the Office of Management and Budget (OMB) on safeguarding PII in the possession of the Federal Government. The NRC issued the policies described below to agency staff through the use of all-employee announcements referred to as "yellow announcements" (YA).

YA 2006-069, "Protection of Personally Identifiable Information," dated September 19, 2006, contained the following directions from the Executive Director for Operations (EDO):

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted.
- Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices.
- Prohibits staff from using personally-owned computers for processing or storing information pertaining to NRC official business that contains the PII of individuals other than themselves.
- Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted.
- Restricts remote access to PII on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout.
- Prohibits e-mail of PII outside of the NRC's infrastructure, except where necessary to conduct agency business.
- Requires managers of Privacy Act systems of records to identify existing extracts or outputs that contain PII and determine whether the extracts are necessary; log all computer-readable data extracts from these systems holding PII and verify that each extract, including PII, has been erased within 90 days or that its use is still required. For systems that cannot automatically generate logs of data extracts, manual logs must be maintained.

YA 2007-096, "Guidance for Periodic Review of Agency Network Drives for the Presence of Personally Identifiable Information," dated September 6, 2007, stated that the NRC would review all agency-shared network drives for the purposes of identifying and eliminating PII at least annually. Each search will begin where the previous search finished. The NRC will review only those files placed on the drive after the end date of the previous search, or previously existing files that were modified after the end date of the previous search.

YA 2007-106, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated September 19, 2007, issued the agency's PII breach notification policy which addresses the security of information systems, whether in paper or electronic form, incident reporting and handling, notification outside the agency, and the responsibilities of individuals who are authorized access to PII. This policy was revised to incorporate credit monitoring services, including the quantitative risk analysis formula, and issued to staff through YA 2009-014, dated February 9, 2009.

YA 2008-021, "Policy Revision: Policy Prohibiting the Use of Peer-to-Peer Software, and Its Impact on Processing Sensitive Unclassified Non-Safeguards Information on NRC Information Technology Systems, Mobile Devices, and Home Computers," dated February 7, 2008, prohibits all employees, including staff and contractors, from installing peer-to-peer software on agency computers without the explicit written approval of an agency Designated Approving Authority. In addition, employees are prohibited from processing sensitive unclassified non-safeguards information (SUNSI) (PII is a sub-set of SUNSI) on home computers unless connected to and working within CITRIX, the NRC broadband remote access system. Employees are prohibited from downloading or storing SUNSI (including PII) to the hard drive of a home computer when connected to and working within CITRIX. Employees are also prohibited expressly from processing SUNSI on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media. Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX or (2) an NRC-issued laptop with NRC-approved encryption software.

YA 2008-063, "Policy: Information Security and Records Management Requirements When Using Information Sharing and Learning Technologies Such As SharePoint and Tomoye," dated April 17, 2008, stated that the following applies to content on sites using these tools:

- SUNSI is prohibited unless appropriate access restrictions are applied on a need-to-know basis.
- PII, which is a subset of SUNSI, is prohibited as stated above, except when the PII is part of a communication on regulatory matters submitted to the NRC by an external entity that is intended for public dissemination (e.g., rulemaking comments or adjudicatory filings).
- Uses of personal sites, such as "My Site" in SharePoint, are restricted to work- and office-related information only. No personal information, including PII, is permitted.

YA 2008-092, "Information Technology Implementation Policy - Computer Security Information Protection Policy," dated June 26, 2008, issued revised policy requiring staff to (1) integrate security and privacy requirements into information system investments and (2) fund security and privacy over the lifecycle of each system undergoing development, modernization, or enhancement. Also, staff must ensure that operational systems meet applicable security requirements for security-significant isolated or widespread weaknesses identified by the agency Inspector General, the Government Accountability Office, or during privacy program reviews.

YA 2008-093, "Information Technology Implementation Policy - Updated Computer Security Incident Response and Personally Identifiable Information Incident Response," dated July 3, 2008, issued revised policy which provides direction for responding to computer security incidents affecting NRC systems, networks, and users, as well as PII incidents. The revised policy contains timeframes for responding to such incidents, based on the criticality of the

affected resources and the incident; formally establishes a Computer Security Incident Response Team (CSIRT) to respond to such incidents; and outlines the CSIRT security incident response process.

YA 2008-126, "Policy Reminder: Personally Identifiable Information and Employee Identification Number," dated September 9, 2008, stated that the NRC no longer treats the employee identification number (EIN) as PII. This enables use of the EIN instead of the Social Security number (SSN) in the e-Travel System, the iLearn Learning Management System, and other NRC uses.

YA 2008-157, "Information Technology Security Policy - Encryption of Data at Rest," dated December 17, 2008, stated that all electronic media containing NRC sensitive information must be encrypted if the media is outside of NRC facilities.

YA 2009-014, "Commission Approves Credit Monitoring Services for Victims of NRC Personally Identifiable Information Breaches," dated February 9, 2009, stated that NRC will offer credit monitoring services under certain circumstances to individuals whose PII has been unintentionally breached by the NRC.

YA 2009-035, "Information Technology Security Policy - Laptop Security Policy," dated April 2, 2009, provides direction for securing laptops.

YA 2012-124, "Computer Security Rules of Behavior Policy," dated October 2, 2012, issued updated agency-wide rules of behavior for authorized computer use which applies to all NRC employees, contractors, vendors, and agents (users) who have access to any system operated by the NRC or by a contractor or outside entity on behalf of the NRC.

2. Reviews Conducted To Identify and Reduce the Unnecessary Collection and Use of PII

To identify and eliminate the unnecessary collection, use, and improper storage of PII, including the SSN, within the agency, the staff has performed the actions described below.

In response to the Office of the Inspector General (OIG) Audit (OIG-06-A-14), "Evaluation of Personal Privacy Information Found on NRC Network Drives", dated June 30, 2006, which found PII on agency-shared network drives, the EDO directed staff to review data generated or stored on the shared network drives for PII. On April 18, 2007, the staff completed the first search of the shared network drives and all identified PII was either removed from the shared drives or access to the PII was restricted to individuals with a need-to-know. The search of the shared network drives has been conducted each year since, with the last one completed in 2011.

On September 29, 2006, in an effort to identify how PII is used in the NRC and to develop policies and procedures to protect PII, the NRC's Senior Agency Official for Privacy established the PII task force. The PII task force began its efforts in October 2006, coordinating with each of the agency's program and support offices, compiling details of the types of PII used throughout the agency, the data sources that contain PII, the forms the agency uses that collect PII, the uses and dissemination of PII, and the methods used to store and safeguard PII. In May 2007, the PII task force began analyzing the information compiled to determine how and where specific uses and collections of the SSN could be reduced or eliminated. As a result of this collaboration, the following actions were taken:

- The Office of Administration (ADM) modified its Dosimeter Tracking System to eliminate the use of the SSN to verify an employee's identity for tracking dosimeters. The employee identification number replaced the SSN in this system.
- The Office of Human Resources (HR) eliminated the use of the SSN on quality assurance reports and on general distribution versions of the Employee Profile Report.
- The Office of the Chief Financial Officer (OCFO) developed a new vendor table that masks all PII in its Federal Financial System. This development was carried forward when the agency upgraded its core financial system in FY 2011 to the Federal Accounting and Integrated Accounting System (FAIMIS). For users needing full access to the vendor table (unmasked) and other tables containing PII, it will be necessary to verify that full access is indeed required because of the user's job description. In addition, the "Official Travel Authorization" form (NRC Form 279), "Travel Voucher" form (NRC Form 64), and the "Claim for Reimbursement for Expenditures on Official Business" form (Standard Form 1164, local travel voucher), no longer require the employee's full SSN. These documents only require the last four digits of the employee's SSN. This minimizes the exposure of the traveler's SSN as travel documents move through the approval, accounting, and payment process.

To eliminate the unnecessary collection of PII, in August 2007 the staff began a review of agency forms that collect information about individuals. The staff reviewed each form in coordination with the sponsoring office to determine if the collection of PII, especially the SSN, was necessary. If the collection of all or part of the PII was determined to be necessary, the requirement to collect the PII, especially the SSN, was identified along with any processes and procedures that should be modified to either reduce access or visually mask the PII. If the staff determined that the collection of part or all of the PII was unnecessary, a decision was made to discontinue the collection or, in the case of the SSN, use another unique identifier. The staff completed this action August 4, 2008. The NRC's forms review process is an ongoing effort to ensure that current and proposed agency forms that collect PII are reviewed to prevent, reduce, or eliminate any unnecessary collections.

On March 26, 2008, the staff received instructions to begin a review of agency administrative office files to eliminate any unnecessary use of and access to PII. For most offices, these are the files that include copies of travel, training, and personnel records generated by the office about its staff. The staff was instructed to (1) reduce the volume of collected and retained information about employees assigned to the office to the minimum necessary, (2) not to collect, use, or retain employees' SSN, (3) limit access to these files, as well as the information from these files, to staff with a need-to-know to perform their assigned duties (official business), and (4) secure paper records in locked file cabinets and password protect electronic records, at a minimum, to make information inaccessible to individuals not authorized access. All offices and regions acknowledged completion of this review by September 9, 2008.

The current network data loss prevention system is now configured to identify and alert when unencrypted SSNs and credit card numbers are traversing the network.

On March 25, 2009, OIS completed the search of the Agencywide Documents Access and Management System (ADAMS) Publicly Available Records System (PARS) for PII and identified 27,983 documents as potentially containing PII. A review of those documents revealed 128 that actually contained PII. The staff redacted all of those documents and placed them back into PARS.

The staff performs routine reviews of the agency's Privacy Act systems of records (SORs). These reviews not only ensure that the notices accurately describe the SORs, but also provide the opportunity to take a fresh look at the types of records being collected about individuals, to remind staff of the agency requirements to protect the records from unauthorized access, and the opportunity to eliminate any unnecessary (no longer required) collections or uses of PII. This review is conducted every 2 years with the last review completed in September 2012.

3. Staff Awareness

To ensure that staff members are familiar with the policies and implementing procedures for the proper protection of PII, routine network announcements and YAs are issued for information and reminder purposes. Other measures to promote staff awareness include the following:

- NRC mandatory annual awareness courses, which address computer security awareness and information security awareness, have been updated to incorporate guidance on the proper handling and protection of PII.
- On November 28, 2006, the NRC introduced the "PII Project" internal Web site to provide the staff with access to OMB's PII guidance, the agency's implementing procedures, and frequently asked questions.
- The SUNSI handling requirements, which are available on the SUNSI internal Web site, were updated to combine PII with the Privacy Act handling group, providing guidance on access, use outside of the agency, transmission, storage, and destruction.
- HR developed labels to be used on locked containers that transport paper records with SSNs.
- The Office of Information Services (OIS), in coordination with the Office of the General Counsel (OGC) and ADM, developed a contract clause for protecting PII that may be provided, collected, used, possessed, or processed in the course of performing work under an NRC contract.
- NRC's "Personally Identifiable Information Responsibilities Awareness and Acknowledgement of Understanding" was released through YA 2009-116, dated November 16, 2009. The staff developed this training presentation in response to OMB M-07-16, to ensure that all personnel are aware of their responsibilities for protecting PII, understand the consequences for violating these responsibilities, and acknowledge this understanding annually. This training is reviewed annually and updated as needed. NRC announcements are issued annually to remind staff of this mandatory training requirement.
- The "Introduction to Controlled Unclassified Information" course was made available to NRC staff April 25, 2011, and the "Introduction to Executive Order 13556: Controlled Unclassified Information (CUI)" course was made available September 20, 2011. These short courses are not mandatory, but all employees and contractors are encouraged to take them to become familiar with CUI, because the NRC is participating in the Federal-wide initiative to implement the CUI program, which will be phased in over the next few years. These courses provide the basics of the Executive Order as well as what to expect next in the CUI implementation process.

4. Guidance for Submitting Documents to the NRC

On March 9, 2007, the staff issued NRC Regulatory Issue Summary (RIS) 2007-04, "Personally Identifiable Information Submitted to the U.S. Nuclear Regulatory Commission." This RIS informs addressees that they should clearly identify documents submitted to the NRC as sensitive if they contain any PII in accordance with Title 10, Section 2.390, "Public Inspections, Exemptions, Requests for Withholding," of the *Code of Federal Regulations* (10 CFR 2.390) so that these documents will not be placed in the Publicly Available Records System (PARS).

5. Actions Taken to Protect PII

Federal Information Processing Standard 140-2 validated, encrypted universal serial bus thumb drives were deployed to staff. This allows authorized staff to securely transport, process, and store electronic PII.

On July 1, 2008, the OCFO started returning processed travel authorizations to all staff in PDF format via e-mail. This paperless delivery better serves all employees, particularly those employees who work away from the Headquarters Complex by eliminating the need for the NRC to fax or mail the paper documents.

The payroll provider for the NRC, the U.S. Department of Interior's National Business Center, has removed or masked the SSN from standard reports and display screens where appropriate. The masking of the SSN on the employee copy of the SF-50 was implemented in April 2009.

NRC developed and implemented a new contract clause entitled "Contractor Responsibility for Protecting Personally Identifiable Information." Since June 16, 2009, the new clause has been inserted in all solicitations and contracts, purchase orders, orders awarded against another government agency's contract, and interagency agreements, where a contract requires contractor access, inadvertent or otherwise, to any form of NRC owned or controlled PII, such as that which may be contained in documents, files, or databases. This clause is used on its own or as a companion clause to FAR clauses 52.224-1 and 52.224-2; and 2) other privacy and security safeguards clauses where the contract requires contractor employee access to such information.

Beginning October 1, 2009, the NRC's eTravel authorization process was condensed down from three levels of approval to two. The eTravel system routes an employee's travel authorization request to the designated travel approving official within their office and then to the designated travel funds certification official. Once these approvals have been completed, the traveler is notified by e-mail that the authorization is complete.

The NRC's conversion to the Office of Personnel Management's Electronic Personnel Folder (e-OPF) was completed in January 2010. The e-OPF eliminates the need for the NRC to file, copy, fax, or mail a majority of the paper personnel documents.

NRC completed the upgrade of SecureZip to the current supported Federal Information Processing Standard (FIPS) 140-2 validated version in November 2010. This upgrade provides further assurance that NRC data that is sent internally or externally, and has been zipped and encrypted with this software, cannot be viewed by anyone for whom it was not intended.

NRC replaced a significant number of standard desktops with mobile desktops (laptops) that employ full disk encryption and have FIPS 140-2 encrypted connectivity to the NRC network via virtual private network so mobile users can securely use laptops at NRC and in remote

locations. The mobile desktop distribution started at the end of FY2010. Over the course of FY2011, more than 550 mobile desktops have been provided to NRC staff.

NRC implemented the Network Access Control system that identifies unauthorized connections to the NRC network and isolates these users on a network where they cannot access any NRC resources, but still allows them access to the Internet, was completed June 2011.

NRC completed the addition of enhancements to Webmail that allow remote users to securely review email attachments in June 2011.

Progress Update on Actions Taken to Protect Personally Identifiable Information/Social Security Numbers

October 5, 2012

U.S. Nuclear Regulatory Commission

Progress Update on Actions Taken to Protect Personally Identifiable Information/Social Security Number

The U.S. Nuclear Regulatory Commission (NRC) has completed all actions identified in its "Plan to Eliminate the Unnecessary Collection and Use of Social Security Numbers," dated September 19, 2007. To build on the efforts identified in this plan, the NRC continues to develop and issue policy and procedures to protect personally identifiable information (PII), which includes the Social Security number (SSN), and to eliminate or reduce its unnecessary collection and use. Below are the actions that have been taken by the NRC to protect PII.

1. Agency Policy Issued on Safeguarding Personally Identifiable Information

The NRC has developed policies and procedures to implement guidance from the Office of Management and Budget (OMB) on safeguarding PII in the possession of the Federal Government. The NRC issued the policies described below to agency staff through the use of all-employee announcements referred to as "yellow announcements" (YA).

YA 2006-069, "Protection of Personally Identifiable Information," dated September 19, 2006, contained the following directions from the Executive Director for Operations (EDO):

- Prohibits the removal of electronic PII from NRC-controlled space until all PII on mobile computers or devices is encrypted.
- Prohibits staff from storing PII pertaining to NRC official business on personally-owned hard drives, removable media, and other stand-alone storage devices.
- Prohibits staff from using personally-owned computers for processing or storing information pertaining to NRC official business that contains the PII of individuals other than themselves.
- Prohibits staff from removing paper documents that contain PII of individuals other than themselves from NRC-controlled space unless the PII has been redacted from the documents or an exception has been granted.
- Restricts remote access to PII on NRC systems by requiring two-factor authentication and enforcing a 30-minute timeout.
- Prohibits e-mail of PII outside of the NRC's infrastructure, except where necessary to conduct agency business.
- Requires managers of Privacy Act systems of records to identify existing extracts or outputs that contain PII and determine whether the extracts are necessary; log all computer-readable data extracts from these systems holding PII and verify that each extract, including PII, has been erased within 90 days or that its use is still required. For systems that cannot automatically generate logs of data extracts, manual logs must be maintained.

YA 2007-096, "Guidance for Periodic Review of Agency Network Drives for the Presence of Personally Identifiable Information," dated September 6, 2007, stated that the NRC would review all agency-shared network drives for the purposes of identifying and eliminating PII at least annually. Each search will begin where the previous search finished. The NRC will review only those files placed on the drive after the end date of the previous search, or previously existing files that were modified after the end date of the previous search.

YA 2007-106, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," dated September 19, 2007, issued the agency's PII breach notification policy which addresses the security of information systems, whether in paper or electronic form, incident reporting and handling, notification outside the agency, and the responsibilities of individuals who are authorized access to PII. This policy was revised to incorporate credit monitoring services, including the quantitative risk analysis formula, and issued to staff through YA 2009-014, dated February 9, 2009.

YA 2008-021, "Policy Revision: Policy Prohibiting the Use of Peer-to-Peer Software, and Its Impact on Processing Sensitive Unclassified Non-Safeguards Information on NRC Information Technology Systems, Mobile Devices, and Home Computers," dated February 7, 2008, prohibits all employees, including staff and contractors, from installing peer-to-peer software on agency computers without the explicit written approval of an agency Designated Approving Authority. In addition, employees are prohibited from processing sensitive unclassified non-safeguards information (SUNSI) (PII is a sub-set of SUNSI) on home computers unless connected to and working within CITRIX, the NRC broadband remote access system. Employees are prohibited from downloading or storing SUNSI (including PII) to the hard drive of a home computer when connected to and working within CITRIX. Employees are also prohibited expressly from processing SUNSI on home computers even when a floppy disk, CD, DVD, or thumb drive is the storage media. Employees who work at home must perform electronic processing of SUNSI on either (1) a home computer within the virtual environment provided by the agency through CITRIX or (2) an NRC-issued laptop with NRC-approved encryption software.

YA 2008-063, "Policy: Information Security and Records Management Requirements When Using Information Sharing and Learning Technologies Such As SharePoint and Tomoye," dated April 17, 2008, stated that the following applies to content on sites using these tools:

- SUNSI is prohibited unless appropriate access restrictions are applied on a need-to-know basis.
- PII, which is a subset of SUNSI, is prohibited as stated above, except when the PII is part of a communication on regulatory matters submitted to the NRC by an external entity that is intended for public dissemination (e.g., rulemaking comments or adjudicatory filings).
- Uses of personal sites, such as "My Site" in SharePoint, are restricted to work- and office-related information only. No personal information, including PII, is permitted.

YA 2008-092, "Information Technology Implementation Policy - Computer Security Information Protection Policy," dated June 26, 2008, issued revised policy requiring staff to (1) integrate security and privacy requirements into information system investments and (2) fund security and privacy over the lifecycle of each system undergoing development, modernization, or enhancement. Also, staff must ensure that operational systems meet applicable security requirements for security-significant isolated or widespread weaknesses identified by the agency Inspector General, the Government Accountability Office, or during privacy program reviews.

YA 2008-093, "Information Technology Implementation Policy - Updated Computer Security Incident Response and Personally Identifiable Information Incident Response," dated July 3, 2008, issued revised policy which provides direction for responding to computer security incidents affecting NRC systems, networks, and users, as well as PII incidents. The revised policy contains timeframes for responding to such incidents, based on the criticality of the

affected resources and the incident; formally establishes a Computer Security Incident Response Team (CSIRT) to respond to such incidents; and outlines the CSIRT security incident response process.

YA 2008-126, "Policy Reminder: Personally Identifiable Information and Employee Identification Number," dated September 9, 2008, stated that the NRC no longer treats the employee identification number (EIN) as PII. This enables use of the EIN instead of the Social Security number (SSN) in the e-Travel System, the iLearn Learning Management System, and other NRC uses.

YA 2008-157, "Information Technology Security Policy - Encryption of Data at Rest," dated December 17, 2008, stated that all electronic media containing NRC sensitive information must be encrypted if the media is outside of NRC facilities.

YA 2009-014, "Commission Approves Credit Monitoring Services for Victims of NRC Personally Identifiable Information Breaches," dated February 9, 2009, stated that NRC will offer credit monitoring services under certain circumstances to individuals whose PII has been unintentionally breached by the NRC.

YA 2009-035, "Information Technology Security Policy - Laptop Security Policy," dated April 2, 2009, provides direction for securing laptops.

YA 2012-124, "Computer Security Rules of Behavior Policy," dated October 2, 2012, issued updated agency-wide rules of behavior for authorized computer use which applies to all NRC employees, contractors, vendors, and agents (users) who have access to any system operated by the NRC or by a contractor or outside entity on behalf of the NRC.

2. Reviews Conducted To Identify and Reduce the Unnecessary Collection and Use of PII

To identify and eliminate the unnecessary collection, use, and improper storage of PII, including the SSN, within the agency, the staff has performed the actions described below.

In response to the Office of the Inspector General (OIG) Audit (OIG-06-A-14), "Evaluation of Personal Privacy Information Found on NRC Network Drives", dated June 30, 2006, which found PII on agency-shared network drives, the EDO directed staff to review data generated or stored on the shared network drives for PII. On April 18, 2007, the staff completed the first search of the shared network drives and all identified PII was either removed from the shared drives or access to the PII was restricted to individuals with a need-to-know. The search of the shared network drives has been conducted each year since, with the last one completed in 2011.

On September 29, 2006, in an effort to identify how PII is used in the NRC and to develop policies and procedures to protect PII, the NRC's Senior Agency Official for Privacy established the PII task force. The PII task force began its efforts in October 2006, coordinating with each of the agency's program and support offices, compiling details of the types of PII used throughout the agency, the data sources that contain PII, the forms the agency uses that collect PII, the uses and dissemination of PII, and the methods used to store and safeguard PII. In May 2007, the PII task force began analyzing the information compiled to determine how and where specific uses and collections of the SSN could be reduced or eliminated. As a result of this collaboration, the following actions were taken:

- The Office of Administration (ADM) modified its Dosimeter Tracking System to eliminate the use of the SSN to verify an employee's identity for tracking dosimeters. The employee identification number replaced the SSN in this system.
- The Office of Human Resources (HR) eliminated the use of the SSN on quality assurance reports and on general distribution versions of the Employee Profile Report.
- The Office of the Chief Financial Officer (OCFO) developed a new vendor table that masks all PII in its Federal Financial System. This development was carried forward when the agency upgraded its core financial system in FY 2011 to the Federal Accounting and Integrated Accounting System (FAIMIS). For users needing full access to the vendor table (unmasked) and other tables containing PII, it will be necessary to verify that full access is indeed required because of the user's job description. In addition, the "Official Travel Authorization" form (NRC Form 279), "Travel Voucher" form (NRC Form 64), and the "Claim for Reimbursement for Expenditures on Official Business" form (Standard Form 1164, local travel voucher), no longer require the employee's full SSN. These documents only require the last four digits of the employee's SSN. This minimizes the exposure of the traveler's SSN as travel documents move through the approval, accounting, and payment process.

To eliminate the unnecessary collection of PII, in August 2007 the staff began a review of agency forms that collect information about individuals. The staff reviewed each form in coordination with the sponsoring office to determine if the collection of PII, especially the SSN, was necessary. If the collection of all or part of the PII was determined to be necessary, the requirement to collect the PII, especially the SSN, was identified along with any processes and procedures that should be modified to either reduce access or visually mask the PII. If the staff determined that the collection of part or all of the PII was unnecessary, a decision was made to discontinue the collection or, in the case of the SSN, use another unique identifier. The staff completed this action August 4, 2008. The NRC's forms review process is an ongoing effort to ensure that current and proposed agency forms that collect PII are reviewed to prevent, reduce, or eliminate any unnecessary collections.

On March 26, 2008, the staff received instructions to begin a review of agency administrative office files to eliminate any unnecessary use of and access to PII. For most offices, these are the files that include copies of travel, training, and personnel records generated by the office about its staff. The staff was instructed to (1) reduce the volume of collected and retained information about employees assigned to the office to the minimum necessary, (2) not to collect, use, or retain employees' SSN, (3) limit access to these files, as well as the information from these files, to staff with a need-to-know to perform their assigned duties (official business), and (4) secure paper records in locked file cabinets and password protect electronic records, at a minimum, to make information inaccessible to individuals not authorized access. All offices and regions acknowledged completion of this review by September 9, 2008.

The current network data loss prevention system is now configured to identify and alert when unencrypted SSNs and credit card numbers are traversing the network.

On March 25, 2009, OIS completed the search of the Agencywide Documents Access and Management System (ADAMS) Publicly Available Records System (PARS) for PII and identified 27,983 documents as potentially containing PII. A review of those documents revealed 128 that actually contained PII. The staff redacted all of those documents and placed them back into PARS.

The staff performs routine reviews of the agency's Privacy Act systems of records (SORs). These reviews not only ensure that the notices accurately describe the SORs, but also provide the opportunity to take a fresh look at the types of records being collected about individuals, to remind staff of the agency requirements to protect the records from unauthorized access, and the opportunity to eliminate any unnecessary (no longer required) collections or uses of PII. This review is conducted every 2 years with the last review completed in September 2012.

3. Staff Awareness

To ensure that staff members are familiar with the policies and implementing procedures for the proper protection of PII, routine network announcements and YAs are issued for information and reminder purposes. Other measures to promote staff awareness include the following:

- NRC mandatory annual awareness courses, which address computer security awareness and information security awareness, have been updated to incorporate guidance on the proper handling and protection of PII.
- On November 28, 2006, the NRC introduced the "PII Project" internal Web site to provide the staff with access to OMB's PII guidance, the agency's implementing procedures, and frequently asked questions.
- The SUNSI handling requirements, which are available on the SUNSI internal Web site, were updated to combine PII with the Privacy Act handling group, providing guidance on access, use outside of the agency, transmission, storage, and destruction.
- HR developed labels to be used on locked containers that transport paper records with SSNs.
- The Office of Information Services (OIS), in coordination with the Office of the General Counsel (OGC) and ADM, developed a contract clause for protecting PII that may be provided, collected, used, possessed, or processed in the course of performing work under an NRC contract.
- NRC's "Personally Identifiable Information Responsibilities Awareness and Acknowledgement of Understanding" was released through YA 2009-116, dated November 16, 2009. The staff developed this training presentation in response to OMB M-07-16, to ensure that all personnel are aware of their responsibilities for protecting PII, understand the consequences for violating these responsibilities, and acknowledge this understanding annually. This training is reviewed annually and updated as needed. NRC announcements are issued annually to remind staff of this mandatory training requirement.
- The "Introduction to Controlled Unclassified Information" course was made available to NRC staff April 25, 2011, and the "Introduction to Executive Order 13556: Controlled Unclassified Information (CUI)" course was made available September 20, 2011. These short courses are not mandatory, but all employees and contractors are encouraged to take them to become familiar with CUI, because the NRC is participating in the Federal-wide initiative to implement the CUI program, which will be phased in over the next few years. These courses provide the basics of the Executive Order as well as what to expect next in the CUI implementation process.

4. Guidance for Submitting Documents to the NRC

On March 9, 2007, the staff issued NRC Regulatory Issue Summary (RIS) 2007-04, "Personally Identifiable Information Submitted to the U.S. Nuclear Regulatory Commission." This RIS informs addressees that they should clearly identify documents submitted to the NRC as sensitive if they contain any PII in accordance with Title 10, Section 2.390, "Public Inspections, Exemptions, Requests for Withholding," of the *Code of Federal Regulations* (10 CFR 2.390) so that these documents will not be placed in the Publicly Available Records System (PARS).

5. Actions Taken to Protect PII

Federal Information Processing Standard 140-2 validated, encrypted universal serial bus thumb drives were deployed to staff. This allows authorized staff to securely transport, process, and store electronic PII.

On July 1, 2008, the OCFO started returning processed travel authorizations to all staff in PDF format via e-mail. This paperless delivery better serves all employees, particularly those employees who work away from the Headquarters Complex by eliminating the need for the NRC to fax or mail the paper documents.

The payroll provider for the NRC, the U.S. Department of Interior's National Business Center, has removed or masked the SSN from standard reports and display screens where appropriate. The masking of the SSN on the employee copy of the SF-50 was implemented in April 2009.

NRC developed and implemented a new contract clause entitled "Contractor Responsibility for Protecting Personally Identifiable Information." Since June 16, 2009, the new clause has been inserted in all solicitations and contracts, purchase orders, orders awarded against another government agency's contract, and interagency agreements, where a contract requires contractor access, inadvertent or otherwise, to any form of NRC owned or controlled PII, such as that which may be contained in documents, files, or databases. This clause is used on its own or as a companion clause to FAR clauses 52.224-1 and 52.224-2; and 2) other privacy and security safeguards clauses where the contract requires contractor employee access to such information.

Beginning October 1, 2009, the NRC's eTravel authorization process was condensed down from three levels of approval to two. The eTravel system routes an employee's travel authorization request to the designated travel approving official within their office and then to the designated travel funds certification official. Once these approvals have been completed, the traveler is notified by e-mail that the authorization is complete.

The NRC's conversion to the Office of Personnel Management's Electronic Personnel Folder (e-OPF) was completed in January 2010. The e-OPF eliminates the need for the NRC to file, copy, fax, or mail a majority of the paper personnel documents.

NRC completed the upgrade of SecureZip to the current supported Federal Information Processing Standard (FIPS) 140-2 validated version in November 2010. This upgrade provides further assurance that NRC data that is sent internally or externally, and has been zipped and encrypted with this software, cannot be viewed by anyone for whom it was not intended.

NRC replaced a significant number of standard desktops with mobile desktops (laptops) that employ full disk encryption and have FIPS 140-2 encrypted connectivity to the NRC network via virtual private network so mobile users can securely use laptops at NRC and in remote

locations. The mobile desktop distribution started at the end of FY2010. Over the course of FY2011, more than 550 mobile desktops have been provided to NRC staff.

NRC implemented the Network Access Control system that identifies unauthorized connections to the NRC network and isolates these users on a network where they cannot access any NRC resources, but still allows them access to the Internet, was completed June 2011.

NRC completed the addition of enhancements to Webmail that allow remote users to securely review email attachments in June 2011.