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

UNITED STATES NUCLEAR REGULATORY COMMISSION

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.