Revised: 2/2014

U.S. NUCLEAR REGULATORY COMMISSION
PERSONALLY IDENTIFIABLE INFORMATION
BREACH NOTIFICATION POLICY

NOTIFICATION POLICY

In accordance with established policy, the U.S. Nuclear Regulatory Commission (NRC) actively protects personally identifiable information (PII) from access by, or disclosure to, unauthorized individuals. The purpose of this document is to reiterate policy and establish standardized response and notification procedures for breaches of that policy. In the event of a breach in PII security requirements, agency personnel are to comply with the following procedures for response and providing notice to affected individuals, other Federal agencies, and the media, as appropriate. These policies and procedures govern breaches by agency personnel—including those that occur through the use of social media—that might result in unauthorized access, either internal or external to the NRC, whether involving electronic or paper documents.

CORE MANAGEMENT GROUP

To review PII breaches and determine the appropriate response thereto, the NRC established a Core Management Group (CMG) consisting of the General Counsel, the Inspector General, the Chief Information Officer (CIO), and the Director of the Office of Information Services (OIS) or their designees. CMG membership may be supplemented as follows:

- For breaches involving current or former employees, the Chief Human Capital Officer (CHCO) and his or her designee will serve on the CMG.

- For breaches affecting contractor personnel, the Director of the Office of Administration (ADM) and the Chief Financial Officer or their designees will serve on the CMG.

- For breaches resulting in a CMG decision to notify affected individuals, the Directors of the Office of Public Affairs and the Office of Congressional Affairs, or their designees, will serve on the CMG.

- For breaches involving information technology systems, the Chief Information Security Officer (CISO), or his or her designee, will serve on the CMG.

TERMINOLOGY

Personally identifiable information (PII) refers to information that can be used to identify or contact a person uniquely and reliably or can be traced back to a specific individual (i.e., a person's name in combination with any of the following information, such as relatives' names, postal address, personal e-mail address, home or cellular telephone number, personal characteristics, Social Security number (SSN), date or place of birth, mother's maiden name, driver's license number, bank account information, credit card information, or any information that would make the individual's identity easily discernible or traceable).

Breach, as directed by OMB Memorandum M-07-16 dated May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," refers to loss of PII control amounting to actual or potential compromise, including: unauthorized disclosure; unauthorized acquisition or access; or any similar situation involving unauthorized use through inappropriate PII access that is (1) potential or confirmed, (2) within the agency or outside the agency, and (3) regardless of format, whether physical (paper) or electronic.

Revised: 2/2014

U.S. NUCLEAR REGULATORY COMMISSION
NOTIFICATION PROCEDURES FOR BREACHES INVOLVING
PERSONALLY IDENTIFIABLE INFORMATION

TABLE OF CONTENTS

U.S. NUCLEAR REGULATORY COMMISSION
PERSONALLY IDENTIFIABLE INFORMATION
BREACH NOTIFICATION PROCEDURES

I. REPORTING OF SUSPECTED OR ACTUAL BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION

A. Immediate Reports

1. To Supervisor and Chief Information Security Officer (CISO)

On the discovery or detection of any incident involving a potential or confirmed breach of PII, within the U.S. Nuclear Regulatory Commission (NRC) or outside the NRC, including unauthorized access to the NRC's local area network (LAN) or applications, and whether in physical (paper) or electronic format, cognizant staff will within one (1) hour report the incident by contacting the Security Incident Hotline at (301)415-6666, option 1 for a physical security incident or option 2 for a computer security incident. Staff may also navigate to the NRC internal website and select "Report a Safety/Security Incident" (http://www.internal.nrc.gov/) at the top right corner of webpage, and follow the appropriate links. After submittal of the initial report, staff must report the incident to their direct supervisory chain. The supervisor receiving the report will promptly verify that an initial report was submitted and notify the Chief Information Security Officer (CISO) or his or her designee in accordance with the established reporting process on the NRC's Internal Web site.

2. To Department of Homeland Security

Within one (1) hour of discovery or detection, the CISO or his or her designee will report any incident described in I.A.1 above to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT), and promptly apprise the Senior Agency Official for Privacy (SAOP) of the notification.

3. To Core Management Group

The SAOP will immediately notify the Core Management Group (CMG) upon receipt of a report of potential or confirmed breach of PII under I.A.1. The CMG will meet as soon as possible, but not later than one day from the date it receives notification.

B. Other Reports

1. To Office of Executive Director of Operations

The Chief Information Officer (CIO) or Deputy CIO or his or her designee will promptly notify the Office of the Executive Director for Operations on receipt of a report of potential or confirmed breach of PII, in accordance with the provisions of Management Directive (MD) 3.4, "Release of Information to the Public."

2. To Office of Inspector General

The CISO or his or her designee will promptly notify the Office of the Inspector General on receipt of a report of potential or confirmed breach of PII, in accordance with the provisions of MD 3.4.

II. BREACH NOTIFICATION

When a suspected or confirmed breach notification has been reported to US-CERT, the CMG will consider six elements in evaluating the situation: (1) whether breach notification is required; (2) timeliness of the notice; (3) responsibility for the notice; (4) contents of the notice; (5) means of providing the notice; (6) and public outreach in response to the notice. In addition to consideration of breach notification, the CMG will ensure that appropriate steps are initiated to mitigate the breach's impact and recurrence, in keeping with NRC and National Institute of Standards and Technology (NIST) guidance.[1]

A. Assessing Need for Breach Notification

To determine whether notification of a breach is required, the CMG must first assess the likelihood of harm occurring and then assess the magnitude of potential harm. The CMG should consider a wide variety of potential harms, such as harm to reputation and the potential for harassment or prejudice, embarrassment, inconvenience, unfairness or theft of identity. In circumstances where notification could increase a risk of harm, the CMG may decide to delay notification while appropriate safeguards are put in place.

In assessing the likely risk of harm, the CMG will consider six additional factors: (1) the nature of the breach; (2) the type of data elements breached; (3) the number of individuals affected; (4) the likelihood that the information is accessible and usable; (5) the likelihood that the breach might lead to harm; and (6) the ability of the NRC to mitigate the risk of harm.

---

[1] NIST Special Publication 800-53 provides a framework for categorizing information and information systems and provides minimum security requirements and minimum security controls for incident handling and reporting. For additional information on NIST guidance and standards, see http://www.nist.gov.

1. Nature of Breach

Several aspects of the breach must be considered in deriving reasonable conclusions about the essential characteristics of the breach, particularly with respect to formulating appropriate steps for corrective or mitigated action. These include questions about the following matters:

(a) Was the LAN, wide area network, or other applications accessed?

(b) Is there any evidence of harm as a result of the breach?

(c) What vulnerability was exploited?

(d) What actions can or should be taken before, or in conjunction with, notification?

2. Type of Data Elements Breached

The type of data elements comprising the breach is a key factor to consider in deciding when and how notification should be provided to affected individuals. For example, theft of a database containing individuals' names in conjunction with SSNs and/or dates of birth might pose a high level of risk of harm, while a theft of a database containing only the names of individuals and residential telephone numbers might pose a lower risk, depending on its context. In assessing the levels of risk and harm, the CMG will consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

3. Number of Individuals Affected by Breach

The CMG will assess the magnitude of the number of affected individuals when determining the method(s) for providing notification. The number of affected individuals will not be the sole determining factor for whether the CMG determines to provide notification. For example, if the breach includes information with a greater potential of harm for only a subset of individuals, notification may be appropriate for only that subset.

4. Likelihood That Information Is Accessible and Usable

The CMG will assess the likelihood that PII will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the CMG's decision whether to provide notification. Increased risk might occur when the benefit, financial or otherwise, of improperly using the information, is tangible and significant.

The fact that the information has been lost or stolen does not necessarily mean that it has been or can be accessed by unauthorized individuals, however,

depending on whether any of a number of physical, technological, or procedural safeguards have been employed to protect the information. For example, if the information is properly protected by encryption, or special software is needed to read or access the data, the risk of compromise must be evaluated. Some encryption affords little or no protection and other encryption protects the information for a period of time. As with all encryption, it is only a matter of time before the information is accessible, and the length of time depends on the strength of the encryption. The CMG will assess whether the PII is at a low, moderate, or high risk of being compromised. This assessment will be guided by the NIST security standards and guidance. Other considerations might include the likelihood that any unauthorized individual will know the value of the information and either use the information or sell it to others.

5. Likelihood That Breach Might Lead to Harm

The CMG will assess the likelihood that a breach might result in harm by considering the manner of the suspected or actual breach and the type(s) of data involved in the incident. The CMG will consider a broad range of potential harms, including embarrassment, inconvenience, unfairness, the effects of a breach of confidentiality or fiduciary responsibility, theft of identity, the potential for blackmail, the disclosure of private facts, mental pain and emotional distress, the potential for secondary uses of the information that could result in fear or uncertainty, or the unwarranted exposure of personal information leading to humiliation or loss of self-esteem.

6. Steps To Minimize Risk of Harm and Mitigate Impact of Breach

The CMG will consider steps that can be taken to mitigate further compromise of the PII and to mitigate any negative results from the breach. For example, within an information system, the risk of harm will depend on whether the NRC is able to mitigate further compromise of the system(s) affected by the breach or to contain the information and limit its dissemination. In addition to containing the breach, appropriate countermeasures should be taken, such as monitoring system(s) for misuse of the PII and patterns of suspicious behavior. Such mitigation might not prevent the use of the personal information for identity theft, but it might limit the associated harm. Some harm might be more difficult to mitigate than others, particularly where it is individualized and the potential injury might be more difficult to determine.

B. Policy and Factors for Notification and Credit-Monitoring Eligibility Determination—Risk Assessment Formula

The six factors mentioned above are applied to the formula described in this section to determine whether to provide breach notification. The CMG will assess risk and harm to the individual and organization for notification purposes and then further determine risk and harm for credit-monitoring purposes. NRC will only provide credit-monitoring

services when the breach occurrence is tied to the NRC's fault or responsibility in causing the breach.

Risk[2] is a function of the probability or likelihood of a privacy violation and the resulting impact[3] of that violation. To assign a risk score, the CMG will assess the probability of the occurrence of the event (data breach) and then assess the potential impact or harm that would be caused to an individual and to the NRC in terms of the agency's ability to achieve its mission. Table 1 provides the definitions for the three risk scores.

Table 1 Likelihood Definitions

Likelihood	Definition
High (H)	The nature of the attack and the data indicate that the motivation is criminal intent; measures to ensure the security of the data and controls to minimize the likelihood of a privacy violation are ineffective.
Medium (M)	The nature of the attack and the data indicate that the motivation could be criminal intent, but controls are in place that might impede success.
Low (L)	The nature of the attack or inadvertent breach and the data do not indicate criminal intent, and security measures and controls are in place to prevent, or at least significantly impede, a privacy violation.

To assess the likelihood of a breach occurring, the CMG will consider the following five factors and assign a score for each factor (High = 3, Medium = 2, Low = 1), total the numbers for all factors, and divide by 5 (rounding up or down):

---

[2] Risk—The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. (Federal Information Processing Standards (FIPS) 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006)

[3] Impact—The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability. (National Institute of Standards and Technology (NIST) Special Publication 800-60, "Guide for Mapping Types of Information and Information Systems to Security Categories," Vol. 1, Rev. 1, August 2008)

(1) how the loss occurred

Factor	Method of Data Loss
High	online system hacked
High	data were targeted
Moderate	device was targeted
Moderate	device stolen
Low	device lost
Low	Inadvertent release/spill

(2) data elements breached (A combination of identifying information and financial or security information should always be considered as high risk with high likelihood of harm occurring.)

Factor	Type of Data
High	Social Security number
High	biometric record
High	financial account number
High	personal identification number (PIN) or security code for financial account
High	health or disability data
High	any combination of identifying information and financial or security information
Moderate	birth date
Moderate	government-issued identification number (e.g., driver's license)
Low	name
Low	address
Low	telephone number

(3) ability to access data

Factor	Ability To Access Data
High	paper records or electronic records in a document that is not encrypted
High	electronic records that have been encrypted using encryption that has not been validated using Federal Information Processing Standard (FIPS) 140
High	electronic records that have been encrypted using weak encryption or using encryption that has been broken
High	electronic records for which the sensitivity does not expire within 5 years (most current encryption will be broken within 5 years)
Moderate	electronic records that do not meet the criteria for high access ability and that have been encrypted using FIPS 140 validated encryption with weaker encryption mechanisms (i.e., password protection, short key lengths encryption not in accordance with required key lengths for information with a moderate confidentiality sensitivity identified in CSO Standard CSO-STD-2009)
Low	electronic records that are encrypted using FIPS 140 validated encryption in accordance with required key lengths for information with a moderate confidentiality sensitivity identified in CSO Standard CSO-STD-2009

(4) ability to mitigate the risk of harm (The basis for this evaluation needs to be documented.)

Factor	Ability To Mitigate Risk of Harm
High	no recovery of paper data
High	recovery of device or data store, but high likelihood that electronic data have been accessed
High	no recovery of device or data store
Moderate	partial recovery of paper data
Moderate	moderate likelihood that electronic data have been or will be accessed
Moderate	recovery of device or data store, but moderate likelihood that electronic data have been accessed
Low	recovery of paper data before use
Low	recovery of device or data store, but low likelihood that electronic data have been accessed

(5) evidence of data being used for identity theft or other harm

Factor	Evidence of Data Use for Malicious Purposes
High	data published on the Web
Moderate	data accessed but no evidence of use
Low	no evidence that data were accessed or used

After evaluating each factor and assigning an overall probability or likelihood of a breach occurring, the CMG will review and assess the impact or harm to an individual or to the NRC. Table 2 defines the impact ratings.

Table 2 Impact Rating Definitions

Impact Rating	Definition
High	Event might (1) result in human death or serious injury or harm to the individual, (2) result in high costs to the organization, or (3) significantly violate, harm, or impede the organization's mission, reputation, or interest.
Medium	Event might (1) result in injury or harm to the individual, (2) result in costs to the organization, or (3) violates, harm, or impede the organization's mission, reputation, or interest.
Low	Event might (1) result in the loss of some tangible organizational assets or resources; or (2) noticeably affect the organization's mission, reputation, or interest.

The impact depends on the extent to which the breach poses a risk of identity theft or other substantial harm to an individual such as through embarrassment, inconvenience, unfairness, harm to reputation, or the potential for harassment or prejudice, particularly when the breach involves information about health or financial benefits information (5 U.S.C. §552a(e)(10)).

C. Assigning Risk Score

The CMG will then assign a risk score. The risk score is determined by cross-referencing the likelihood score with the impact score using Table 3.

Table 3 Risk Scores

Likelihood	Impact		
	Low	**Medium**	**High**
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

D. Notification

The risk score assigned will help determine whether and when the NRC should provide notification. Notification is provided when the risk score is medium or high. If the likelihood of harm is low, there could be more harm to or impact on the individual if notification is provided because of the actions the notified individual might take. Thus, notification must be weighed with the likelihood of harm. No notification is required when the risk levels for each of the five factors are low. If the five factors are considered appropriately, notification will be given only in those instances where there is a medium or high risk of harm. If the factors are not uniform within a group of affected individuals, then notification may be appropriate for a subset of the group. Therefore, consideration should be given to all factors when determining final actions to take when addressing each incident, as illustrated in Table 4.

Table 4 Action

Risk Score	Necessary Action
High	notify and provide remedy
Medium	notify only
Low	monitor only

E. Notification of Credit-Monitoring Remedy

The notification of a breach will include the option of credit monitoring when the risk score is high. The NRC will invoke a General Services Administration blanket purchase agreement (BPA) or contract with a credit-monitoring company outside the BPA to provide this service.

F. Timeliness of Notification

When the CMG determines that notification is appropriate, in addition to the reporting required by I.A and B, the NRC will notify the affected individual(s) promptly. The staff will take reasonable (but persistent) steps to locate and notify the affected individual(s). In some circumstances, law enforcement or national security considerations might

require a delay if it would seriously impede the investigation of the breach or the affected individual(s). The CMG may delay notification for reasons consistent with the needs of law enforcement and national security and with any measures necessary to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the compromised computerized system. In most cases, any affected individuals will receive prompt notification once the CMG has determined to provide notice regarding the breach. However, the CMG will be careful not to allow any delay that will exacerbate risk or harm to any affected individuals.

G. Responsibility for Breach Notification

In coordination with ADM and OIS, the Director of the NRC program office responsible for the breach will issue the breach notification to the affected individual(s), unless other instructions are given by the CMG. For breaches arising from regional offices, the regional administrator will issue the breach notification, with appropriate coordination.

H. Contents of Notice

The agency will provide notification in writing and employ concise, plain language. The notice should include the following elements:

(1) a brief description of what happened, including the date(s) of the breach and the date of its discovery

(2) to the extent possible, a description of the types of PII, but not the specific PII, involved in the breach (e.g., the full name, SSN, date of birth, home address, or account number would not be provided in the notification)

(3) a statement about whether the information was encrypted or protected by other means, when it is determined that such information would be beneficial and would not compromise the security of the system

(4) the steps an individual should take to protect herself or himself from harm, if any

(5) what the NRC is doing, if anything, to investigate the breach (unless law enforcement or national security agencies have requested that no information be provided about such investigation), mitigate losses, and protect against similar or additional breaches

(6) agency contacts for more information, including a toll-free telephone number, e-mail address, and postal address

(7) if the breach includes financial information, an advisory that the individual should contact her or his financial institution(s) to determine whether the account(s) should be closed

(8) if the breach includes information that can be used to open a new credit account, include:

(a) either how to request a free annual credit report (available at http://www.AnnualCreditReport.com or by calling 1-877-322-8228) or specific information on how to obtain NRC funding for credit monitoring of an affected individual if the CMG determines that it is authorized by law and appropriate

(b) a recommendation that the individual place an initial fraud alert on credit reports maintained by the three major credit bureaus

(c) an advisory that an affected individual should monitor her or his financial account statements and immediately report any suspicious or unusual activity to the responsible financial institution

(d) for a resident of a State with a law that authorizes a credit freeze, a recommendation that the individual consider placing a credit freeze on her or his credit file (State laws vary with respect to usability and cost issues, which individuals will need to consider before deciding to place a credit freeze.)

I. Means of Providing Notification

The best means of providing notification will depend on the number of people affected and what contact information is available for the affected individual(s). The means of providing notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The CMG may consider the following means of notification: (1) telephone, (2) first-class mail, (3) e-mail, (4) substitute notice (see below), (5) newspapers or other public media outlets, (6) existing Government-wide services, and (7) accommodations in accordance with Section 508 of the Rehabilitation Act.

1. Telephone

Telephone notification might be appropriate in those cases where urgency might dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be followed with written notification by first-class mail.

2. First-Class Mail

First-class mail notification to the last known mailing address of the individual in the NRC's records should be the primary means of notification. If there is reason to believe a person's address is no longer current, reasonable steps should be taken to update the address by consulting with other agencies such as the

U.S. Postal Service (USPS) or the Internal Revenue Service (IRS). The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If another agency is used to facilitate mailing (e.g., if the NRC consults with the USPS or IRS for current mailing addresses of affected individuals), care should be taken to ensure that the NRC is identified as the sender and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its content (e.g., "Data Breach Information Enclosed") and should be marked with the NRC as the sender to reduce the likelihood that the recipient assumes it is advertising or "junk" mail.

3. E-mail

E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. While notification by postal mail is preferable, notification by e-mail might be appropriate if an individual has provided an e-mail address to the NRC and has expressly given consent to e-mail as the primary means of communication with the NRC, and no known mailing address is available. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the NRC's public Web site, where notices may be "layered" so the most important summary facts are up front with additional information provided under link headings. Encryption should be employed when its use does not present decryption difficulties for the intended audience. The CMG will determine whether establishing a notice on the NRC's public Web site is appropriate.

4. Existing Government-Wide Services

The NRC may use Government-wide services already in place to provide support services needed, such as USA Services, including the toll-free number of 1-800-FedInfo and the URL http://www.USA.gov.

5. Newspapers or Other Public Media Outlets

The NRC may supplement individual notification by placing notices in newspapers or other public media outlets. The CMG may elect to set up a toll-free call center staffed by trained personnel to handle inquiries from the affected individuals and the public.

6. Substitute Notice

Substitute notice may be used when the NRC does not have sufficient contact information to provide individual notification. Substitute notice should consist of a conspicuous posting of the notice on the NRC public Web site and notice to major print and broadcast media, including media in areas where the affected individuals reside, if known. The notice to the media should include a toll-free

phone number where an individual can learn whether or not his or her personal information is included in the breach.

7. Accommodations under Section 508 of Rehabilitation Act

When providing notice, the agency will give special consideration to individuals who are visually or hearing impaired in ways consistent with Section 508 of the Rehabilitation Act of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf or posting a large-type notice on the NRC public Web site.

J. Public Outreach in Response to Breach

The CMG will determine the appropriate composition of the audience to receive breach notification. The intended audience may include not only the affected individuals, but also third parties affected by the breach, as well as the media.

1. Public Notice

If the CMG determines that it is appropriate to include the public in the intended audience, the agency must carefully plan and execute the public notice so that the notice itself does not unnecessarily alarm the public. When appropriate, the agency should notify the public media as soon as possible after a breach has been discovered and the response plan, including the notice, has been developed. The staff should focus on providing information, including links to resources, to aid the public in its response to the breach. Public notice may be delayed on the request of law enforcement or national security agencies. Prompt public media disclosure is generally preferable because delayed notice will erode public trust.

2. Web Posting

If the CMG determines that it is appropriate to provide information online, the agency will post the information about the breach and provide the notice in a clearly identifiable location on the NRC public Web site as soon as possible. The posting should include a link to frequently asked questions and other information to assist the public's understanding of the breach and the notification process. The information should also appear on the USA Services Web site at http://www.USA.gov. The CMG may also consult with the General Services Administration's USA Services regarding the use of its call center.

3. Other Public and Private Sector Agencies

The CMG will determine whether other public and private sector agencies need to be notified on a need-to-know basis, particularly those that might be affected by the breach or might play a role in mitigating the potential harm stemming from the breach.

4. Inquiries from Congress and Other Agencies

The CMG should be prepared to respond to inquiries from the Congress and other government agencies such as the Government Accountability Office.

III. REASSESSMENT OF BREACH IMPACT LEVEL

After evaluating the reported incident in relation to all the above factors, the CMG will reassess the level of impact already assigned to the information using the impact levels defined by the NIST. This reassessment is important because the security categorization of any breach might need to be altered from the original designation. The impact levels—low, moderate, and high—describe the (worst-case) potential impact on the NRC or any affected individuals if a security breach occurs.

Where a range of risk levels is attributed to the factors, the CMG will decide on the intended audience for the notice by giving greater weight to the likelihood that the information is accessible and useable and that the breach might lead to harm.

A. Low

Loss of confidentiality is expected to have a limited adverse effect on individuals.

B. Moderate

Loss of confidentiality is expected to have a serious adverse effect on individuals.

C. High

Loss of confidentiality is expected to have a severe or catastrophic adverse effect on individuals.

IV. STAFF TRAINING AND RELATED ACTIONS

OIS will train the NRC staff on how to prevent incidents, and on their roles and responsibilities for responding to incidents should they occur, as part of the NRC's annual Information Technology Users' Roles and Responsibilities training. OIS will issue an annual announcement to the NRC staff and on-site contractor personnel reminding them of their roles and responsibilities regarding PII.

OCHCO will manage a program to ensure annual certification of all employees and contractor personnel and will ensure that all NRC staff annually sign a document clearly describing their responsibilities. With the assistance of OIS, OCHCO will develop an NRC form for the annual

certification. OCHCO will include a PII instruction segment during employee initial orientation and obtain each employee's signature on their certification form.

ADM's Division of Contracts will include a PII security provision in all contracts where it is expected that contractor personnel will receive, process, or possess PII.

V. VIOLATIONS

In accordance with the existing authority, the NRC may impose progressive disciplinary measures on employees for infractions of agency PII policy. The following may constitute a basis for disciplinary action, including reprimand, suspension, removal, or other actions consistent with applicable law and policy.

A. Security Controls

Failure of the responsible employee to implement and maintain applicable PII security controls of which the employee is aware, regardless of whether such action results in the loss of control or unauthorized disclosure of PII.

B. Unauthorized Disclosure

Deliberate unauthorized disclosure of PII to others may constitute a basis for disciplinary action. Infractions involving Privacy Act violations (willful disclosure of Privacy Act information to any unauthorized recipients) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

C. Unauthorized Access

Deliberate unauthorized access to or solicitation of PII may constitute a basis for disciplinary action. Infractions involving Privacy Act violations (requests for access to Privacy Act information under false pretenses) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

In addition, appropriate legal action may be pursued for breaches of NRC PII caused by people who are not NRC employees.

D. Reporting Requirements

Failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information may constitute a basis for disciplinary action.

E. Supervision and Training

Failure, as a manager, to adequately instruct, train, or supervise employees in their responsibilities may constitute a basis for disciplinary action.

VI. PRIVACY ACT ROUTINE USE

To enhance the NRC's prompt and effective management of a breach of PII maintained within a Privacy Act system of records, the NRC published a Routine Use for its Systems of Records, effective September 12, 2007. This routine use was established under 5 U.S.C. §552a(b)(3) of the Privacy Act to authorize the disclosure of PII, as necessary, in order to manage a breach.

VII. REFERENCES

A. Statutes

Federal Information Security Management Act of 2002, 44 U.S.C. §3541, et seq.

Freedom of Information Act, 5 U.S.C. §552, as amended

Privacy Act of 1974, 5 U.S.C. §552a

Rehabilitation Act of 1973, 29 U.S.C. §794d

B. Government-Wide Guidance

Office of Management and Budget, OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," Washington, DC, May 22, 2007. Available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf (accessed on February 22, 2014).

Office of Management and Budget, OMB Memorandum M-06-19, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments," Washington, DC, July 12, 2006. Available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m06-19.pdf (accessed on February 22, 2014).

Office of Management and Budget, OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," Washington, DC, May 22, 2006. Available at http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf (accessed on February 22, 2014).

C. Agency Guidance

U.S. Nuclear Regulatory Commission, "Release of Information to the Public," Management Directive (MD) 3.4, February 6, 2009, Agency-wide Documents Access and Management System (ADAMS) Accession No. ML080310417.

U.S. Nuclear Regulatory Commission, "Facility Security Program," MD 12.1, September 14, 2011, ADAMS Accession No. ML102560389.

U.S. Nuclear Regulatory Commission, "NRC Cyber Security Program," MD 12.5, August 15, 2013, ADAMS Accession No. ML122210013.

U.S. Nuclear Regulatory Commission, "NRC Sensitive Unclassified Information Security Program," MD 12.6, December 20, 1999, ADAMS Accession No. ML041700603.

U.S. Nuclear Regulatory Commission, "Information Technology Security Policy - Encryption of Data at Rest," NRC Yellow Announcement (YA)-08-0157, December 17, 2008.

U.S. Nuclear Regulatory Commission, "Information Technology Implementation Policy - Updated Computer Security Incident Response and Personally Identifiable Information Incident Response," NRC YA-08-0093, July 3, 2008.

U.S. Nuclear Regulatory Commission, "Information Technology Implementation Policy - Computer Security Incident Response and Personally Identifiable Information Incident Response," NRC YA-08-0070, May 2, 2008.

U.S. Nuclear Regulatory Commission, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information," NRC YA-07-0106, September 19, 2007.

U.S. Nuclear Regulatory Commission, "Privacy at the NRC," NRC YA-07-0071, July 18, 2007.

U.S. Nuclear Regulatory Commission, "Protection of Personally Identifiable Information," NRC YA-06-0069, September 19, 2006.

U.S. Nuclear Regulatory Commission, "Inadvertent Release of Classified or Sensitive Unclassified Information," NRC YA-03-0037, May 20, 2003, ADAMS Accession No. ML052200275.

U.S. Nuclear Regulatory Commission, "Sensitive Unclassified Information," NUREG/BR-0268, December 1999.

D. Intranet

http://www.internal.nrc.gov/PII/releases.html

http://www.internal.nrc.gov/PII/

VIII. ABBREVIATIONS AND ACRONYMS

ADM	Office of Administration
BPA	blanket purchase agreement
CHCO	Chief Human Capital Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMG	Core Management Group
FIPS	Federal Information Processing Standard
IRS	Internal Revenue Service
LAN	local area network
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	U.S. Nuclear Regulatory Commission
OCHCO	Office of the Chief Human Capital Officer
OIS	Office of Information Services
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIN	personal identification number
SAOP	Senior Agency Official for Privacy
SSN	Social Security number
U.S.C.	*United States Code*
US-CERT	United States Computer Emergency Readiness Team
USPS	U.S. Postal Service

YA Yellow Announcement