September 19, 2007

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 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 notice to affected individuals, other Federal agencies, and the media, as appropriate. These policies and procedures govern breaches by agency personnel that may result in unauthorized access, either internal or external to the NRC, whether involving electronic systems or paper documents.

CORE MANAGEMENT GROUP

To review PII breaches and determine 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 Director of the Office of Human Resources (OHR) 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, 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 (1) potential or confirmed; (2) within the agency or outside the agency; and (3) regardless of format, whether physical (paper) or electronic.

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

TABLE OF CONTENTS

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

I. REPORTING BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION

A. Immediate Reports

1. To Supervisor and Chief Information Security Officer

Upon discovery or detection, cognizant staff will immediately report to direct supervisory chain any incident involving a potential or confirmed breach of PII, within the NRC or outside the NRC, including unauthorized access to the NRC local area network (LAN) or applications, and whether in physical (paper) or electronic format. The supervisor receiving the report will promptly notify the Chief Information Security Officer (CISO), or his or her designee, in accordance with the established reporting process on the NRC Internal Web site.

2. To Department of Homeland Security

Within 1 hour of discovery or detection, the CISO will report any incident described in 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 CMG upon receipt of a report of potential or confirmed breach of PII under 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 CIO, Deputy CIO, or his or her designee, will promptly notify the Office of the Executive Director for Operations upon 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 upon receipt of a report of potential or confirmed breach of PII, in accordance with the provisions of MD 3.4, "Release of Information to the Public."

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: whether breach notification is required; timeliness of the notice; responsibility for the notice; contents of the notice; means of providing the notice; 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 impact and recurrence, consistent with NRC and National Institute of Standards and Technology (NIST) guidance.

A. Assessing Need for Breach Notification

To determine whether notification of a breach is required, the CMG must first assess the likely risk of harm caused by the breach and then assess the level of risk. The CMG should consider a wide variety of 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 data elements breached; (3) the number of individuals affected; (4) the likelihood the information is accessible and usable; (5) the likelihood the breach may lead to harm; and (6) the ability of the NRC to mitigate the risk of harm.

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 mitigative action. These include questions about the following matters:

a. were 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 prior to, or in conjunction with notification?

2. Type of Data Elements Breached

The type of data elements compromising 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 may pose a high level of risk of harm, while a theft of a database containing only the names of individuals and residential telephone numbers may 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.

4. Likelihood 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 may 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 it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed. For example, if the information is properly protected by encryption, or a special software is needed to read or access the data, the risk of compromise may be low to non-existent. 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 may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

5. Likelihood Breach May Lead to Harm

The CMG will consider a broad range of potential harm 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 which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem. The CMG will assess the likelihood that a breach may result in harm by considering the manner of the suspected or actual breach and the type(s) of data involved in the incident.

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. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the PII and patterns of suspicious behavior, should be taken. Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

B. Timeliness of Notification

When the CMG determines notification is appropriate, in addition to the reporting required by 1.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 may require a delay if it would seriously impede the investigation of the breach or the affected individual(s). The CMG may delay notification consistent with the needs of law enforcement and national security and any measures necessary to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized system compromised. In most cases, an affected individual(s) 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 individual(s).

C. Responsibility for Breach Notice

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, pursuant to appropriate coordination.

D. 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., full name, SSN, date of birth, home address, account number)

3. a statement whether the information was encrypted or protected by other means, when determined 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 no information be provided, 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. 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.)

E. Means of Providing Notice

The best means of providing notification will depend upon the number affected and what contact information is available about 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; (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 may be appropriate in those cases where urgency may 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. Where there is reason to believe the 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., the NRC consults with the USPS or IRS for current mailing addresses of affected individuals), care should be taken to ensure 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 the recipient thinks 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 may be appropriate where 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 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 in situations when use does not present decryption difficulties for the intended audience. The CMG will determine whether establishing a notice on the NRC 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 http://www.USA.gov.

5. Newspapers or Other Public Media Outlets

The NRC may supplement individual notification with placing notifications 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 notification. Substitute notice should consist of a conspicuous posting of the notice on the NRC public Web site and notification 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 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.

F. 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. Notification may be delayed upon the request of law enforcement or national security agencies. Prompt public media disclosure is generally preferable because delayed notification 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 talking points 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 Service 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 may be affected by the breach or may 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 as the security categorization of any breach may 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 affected individual(s) if a security breach occurs.

Where there is a range of risk levels attributed to the factors, the CMG will decide on the intended audience for the notice by giving greater weight to the likelihood the information is accessible and useable and whether the breach may 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

OIS will train the NRC staff on how to prevent incidents, and 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. ADM, Division of Contracts will include a PII security provision in all contracts requiring contractor personnel to receive, process, or possess PII. OHR will manage the annual certification program to ensure annual certification of all employees and contractor personnel and ensure that all NRC staff annually sign a document clearly describing their responsibilities.

With the assistance of OIS, OHR will develop an NRC form for the annual certification and will include a PII segment during employee initial orientation and obtain signature on the certification form.

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. In addition, appropriate legal action may be pursued for breaches of NRC PII caused by other than NRC employees.

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 Access

Deliberate, unauthorized access to, or solicitation of, PII. Infractions involving Privacy Act violations (unauthorized access, or requests for access, to Privacy Act information) 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 Disclosure

Deliberate, unauthorized disclosure of PII to others. Infractions involving Privacy Act violations (unauthorized access, or requests for access, to Privacy Act information) may result in criminal prosecution under the Privacy Act. The potential criminal penalties consist of incarceration and monetary fines up to $5,000.

D. Reporting Requirements

Failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information.

E. Supervision and Training

Failure, as a manager, to adequately instruct, train, or supervise employees in their responsibilities.

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, 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

OMB Memorandum M-07-16 dated May 22, 2007, Subject: "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"

OMB Memorandum M-06-19 dated July 12, 2006, Subject: "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments"

OMB Memorandum M-06-15 dated May 22, 2006, Subject: "Safeguarding Personally Identifiable Information"

C. Agency Guidance

Management Directive 3.4, "Release of Information to the Public"

Management Directive 12.1, "Facility Security Program"

Management Directive 12.6, "NRC Sensitive Unclassified Information Security Program"

NRC Announcement No. 2006-069 dated September 19, 2006, Subject: "Protection of Personally Identifiable Information"

NRC Announcement No. 2003-037 dated May 20, 2003, Subject: "Inadvertent Release of Classified or Sensitive Unclassified Information"

NUREG/BR-0268, "Sensitive Unclassified Information"

"Minimum Requirements for Handling Classified and Sensitive Unclassified Information" (yellow card available in NRC Supply Store)

D. Intranet

http://www.internal.nrc.gov/ois/it-security/Inadvertent_Releases.html

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

VIII. ACRONYMS

ADM: Director of the Office of Administration

CIO: Chief Information Officer

CISO: Chief Information Security Officer

CMG: Core Management Group

IRS: Internal Revenue Service

LAN: Local Area Network

NIST: National Institute of Standards and Technology

NRC: Nuclear Regulatory Commission

OHR: Office of Human Resources

OIS: Office of Information Services

PII: Personally Identifiable Information

SAOP: Senior Agency Official for Privacy

SSN: Social Security number

US-CERT: United States Computer Emergency Readiness Team

USPS: U.S. Postal Service