Breach Notification Plan
U.S. Nuclear Regulatory Commission (NRC)
Privacy Program

Office of the Chief Information Officer (OCIO)

Version 2.3

March 18, 2025

Document Revision History

Date	Version	Description	Author
March 18, 2025	2.3	Annual review-updates to credit monitoring services	NRC Privacy Office Oasis Systems, LLC
March 18, 2025	Draft of 2.3	Annual review-updates to credit monitoring services	NRC Privacy Office Oasis Systems, LLC
December 18, 2024	2.2	Revised risk rating criteria	NRC Privacy Office
February 29, 2024	2.1	Final Release	NRC Privacy Office Oasis Systems, LLC
February 07, 2024	Draft of 2.1	Annual Review-minor edits	NRC Privacy Office Oasis Systems, LLC
May 10, 2023	2.0	Final Release	NRC Privacy Office
March 1, 2023	2.0	Major revisions based on new processes and requirements	NRC Privacy Office Oasis Systems, LLC
February 13, 2023	Draft of 2.0	Major revisions based on new processes and requirements	NRC Privacy Office Oasis Systems, LLC
February 2014	1.0	Initial Release	NRC Privacy Office

Table of Contents

Background

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):

Date or place of birth	Relatives' names	Biometric record
Home address	Home telephone number	Bank account pin or security code
Social security number	Personal cellular number	Credit card information
Personal characteristics	Mother's maiden name	Bank account number
Personal email address	Medical or disability information	Driver's license number

A comprehensive listing of PII is provided for further reference in ADAMS at the following link:

PII Reference Table

A privacy breach, as defined by Office of Management and Budget (OMB) Memorandum M-07-16, *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 access, unauthorized modification or deletion, 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. The Nuclear Regulatory Commission (NRC) has a duty to appropriately safeguard PII in its possession and to prevent its compromise to maintain the public's trust.

Breaches involving PII can receive considerable media attention, which can greatly harm an agency's reputation and reduce the public's trust in the organization. Moreover, affected individuals can be subject to embarrassment, identity theft, or blackmail as the result of a breach involving PII.

Per OMB-M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information,* the NRC added a Routine Use to all its Privacy Act system of records notices (SORNs) to enhance the prompt and effective management of a breach impacting PII that is maintained within a Privacy Act system of records.

*A*ll SORNs include routine uses for the disclosure of information necessary to respond to a breach either of the agency's PII or, as appropriate, to assist another agency in its response to a breach.

1 Purpose

A Breach Response Plan is a formal document that includes the agency's policies and procedures for reporting, investigating, and managing a PII breach.

The purpose of the NRC Breach Notification Plan is to inform NRC employees and contractors of the standardized processes and procedures in place for responding to a potential PII breach.

In addition, this plan sets out the roles and responsibilities for reporting and responding to PII breaches so that agency officials, employees, and other individuals may respond quickly and effectively to a breach.

2 Roles and Responsibilities

Table 2-1 identifies the roles and responsibilities of all parties involved in the handling of a potential PII breach.

Table 2-1: Roles and Responsibilities

Role	Breach Responsibilities
Senior Agency Official for Privacy (SAOP)	➢ Notifies the Core Management Group (CMG) upon receiving a report of potential or confirmed breach of PII with a moderate or high-risk determination ➢ Makes final decisions to address agency breaches with a low-risk determination ➢ Ensures prompt notifications are provided to those impacted by the breach ➢ Ensures all recommended actions to address a confirmed breach are implemented ➢ Notifies the appropriate Congressional Committees of a major incident no later than seven days after the date of determination
Core Management Group The CMG is made up of the following roles and/or designees: ➢ SAOP ➢ General Counsel ➢ Inspector General ➢ CIO/Director of OCIO The CMG membership may be supplemented by the following roles and/or designees: ➢ For breaches involving current or former employees, the Chief Human Capital Officer (OCHCO) or designee will serve on the CMG	➢ Reviews the draft risk analysis provided by the SAOP for breaches with a moderate or high-risk determination ➢ Based on the risk analysis, the CMG decides whether a notification letter alone is sufficient or if additional measures, such as offering credit monitoring services, are necessary to protect affected individuals.

Table 2-1: Roles and Responsibilities

Role	Breach Responsibilities
➢ For breaches affecting contractor personnel, the Director of the Office of Administration (ADM) and the Chief Financial Officer (CFO) or designee will serve on the CMG ➢ For breaches resulting in a CMG decision to notify affected individuals, the Directors of the Office of Public Affairs (OPA) and the Office of Congressional Affairs (OCA), or designee, will serve on the CMG For breaches involving information technology systems, the CISO, or designee, will serve on the CMG	
Privacy Officer	➢ Advises the SAOP on progress of breach activities ➢ Creates the draft risk analysis and provides it to the SAOP ➢ Manages notification activities; conducts any necessary and appropriate follow-up ➢ Creates the final risk analysis based on SAOP and CMG recommendations ➢ Contacts Division of Resource Management and Administration (DRMA) for credit monitoring services
Computer Security Incident Response Team (CSIRT)	➢ Conducts initial forensics to confirm the sensitivity of the information ➢ Reports breaches of sensitive PII to the NRC Privacy Officer, Network and Security Operations Branch (NSOB) Chief and the Cybersecurity and Infrastructure Security Agency (CISA) United States Computer Emergency Readiness Team ➢ Any spill that compromises the confidentiality, integrity, and/or availability of NRC systems must be reported to CISA within one hour of identification ➢ Creates the PII Incident Information Report and provides it to the NRC Privacy Officer ➢ Secures the information to avoid further spills ➢ Verifies that appropriate records are maintained to document the initial analysis of the suspected breach and the agency's overall response in all phases of the incident management process
Security Operations Branch (SOB) Chief	➢ Notifies the Chief Information Security Officer (CISO) of possible PII breaches ➢ Provides oversight and guidance for CSIRT activities
Chief Information Security Officer (CISO)	➢ Ensures that PII issues raised by the SOB Chief are addressed

Table 2-1: Roles and Responsibilities

Role	Breach Responsibilities
	➢ Notifies Chief Information Officer (CIO) depending upon the nature of the breach ➢ Advises CMG on the cybersecurity implications of possible or confirmed breaches and spills
Chief Information Officer (CIO)	➢ Notifies the Office of the Executive Director for Operations upon receiving a report of potential or confirmed breach of PII
Office of the Chief Financial Officer (OCFO)	➢ Funds the credit monitoring service
Office of the Chief Information Officer (OCIO) Division of Resource Management and Administration (DRMA)	➢ Administers the credit monitoring contract ➢ Submits requisition in STAQS initiating request for contract actions ➢ Requests funding from OCFO ➢ Engages the contractor to set up credit monitoring services ➢ Provides necessary enrollment instructions for credit monitoring services for those impacted by the breach
Office of Administration	➢ Awards the task order for credit monitoring services

3 Reporting of Suspected or Actual Breach of PII

It is NRC policy that all NRC staff and contractors immediately upon discovery, report any suspected or confirmed breach of PII to the Computer Security Incident Response Team (CSIRT) at CSIRT@nrc.gov or 301-415-6666, along with their direct supervisory chain of command. This includes **but is not limited to**:

- Email spills that may contain PII
- PII spills on Shared Drives, ADAMS, OneDrive, Teams, SharePoint Online, Power Apps
- Stolen/lost/missing NRC laptops or mobile devices that may contain PII

CSIRT conducts initial forensics to confirm the sensitivity of the information and contacts the NRC Privacy Officer to validate that the information is in fact PII. In some cases, a user may inadvertently publish PII that is not exclusively their own. Once CSIRT is made aware of the possible spill, CSIRT requests the Customer Service Center (CSC) to lockdown the file, if applicable, and grant access only to the CSIRT Team and the NRC Privacy Officer to corroborate if it is a PII spill.

Note: Non-electronic PII incidents such as the improper handling or storage (no IT equipment/system involved) of PII must be reported immediately to the Office of Administration (ADM) Division of Facilities & Security (DFS).

Within one (1) hour of discovery or detection, CSIRT will notify the Cybersecurity and Infrastructure Security Agency (CISA) United States Computer Emergency Readiness Team if the confirmed spill compromised the confidentiality, integrity, or availability of NRC systems.

If the NRC determines that a breach constitutes a “major incident,’’ the SAOP will notify the appropriate Congressional Committees no later than seven days after the date of determination. In addition, NRC will supplement their initial seven-day notification to Congress with a report no later than 30 days after the agency discovers the breach.

As defined in OMB-M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, a breach constitutes a "major incident" when it involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification, unauthorized deletion, unauthorized exfiltration, or unauthorized access to 100,000 or more individuals' PII automatically constitutes a "major incident. "

4 Factors that may Influence the Risk Determination for a Breach

After the Privacy Officer receives the CSIRT Report confirming there was a breach, a risk determination must be conducted. Determining risk is a combination of analyzing the likelihood that a privacy violation has been, or will be, exploited and the resulting impact/harm of the violation.

The NRC considers any and all risks relevant to the breach. Consistent with OMB-M-17-12, the factors listed below are considered (as applicable) when assigning an overall risk rating for a specific breach.

Data Elements

Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual.

The NRC evaluates the sensitivity of PII data and how easily the PII can be used to identify individuals. For example, PII data composed of individuals’ names, fingerprints, or SSNs uniquely and directly identify individuals, whereas PII data composed of individuals’ ZIP codes and dates of birth can indirectly identify individuals or can significantly narrow large datasets. However, data composed of only individuals‘ area codes and race usually would not provide for direct or indirect identification of an individual depending upon the context and sample size. Therefore, PII that is uniquely and directly identifiable may warrant a higher impact level than PII that is not directly identifiable by itself.

Context of Use

The purpose or context of use for which PII is collected, stored, used, processed, disclosed or disseminated is taken into account to understand how the disclosure of PII could cause harm to individuals or the agency. This is critical because information that is situated in one context can reveal additional information about an individual that the same information in a different context would not. For example, a list of names and cell phone numbers of agency employees may not, ordinarily, be particularly sensitive. But if the list is a list of agency employees who hold sensitive law enforcement positions, and if an unauthorized individual obtaining access to the list as a result of the breach could

recognize it as such, the names and cell phone numbers would be sensitive, given the context.

Vulnerable Populations

When assessing the nature and sensitivity of PII potentially compromised by a breach, the NRC shall consider whether the potentially affected individuals are from a particularly vulnerable population that may be at greater risk of harm than the general population. Potentially vulnerable populations include but are not limited to: children; active duty military; government officials in sensitive positions; senior citizens; individuals with disabilities; confidential informants; witnesses; certain populations of immigrants; non-English speakers; and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking.

Private Information

The NRC evaluates the extent to which the PII constitutes information that an individual would generally keep private. Such "private information" may not present a risk of identity theft or other criminal conduct but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. Examples of private information include:

- derogatory personnel or criminal information
- personal debt and finances
- medical conditions
- treatment for mental health
- pregnancy related information including pregnancy termination
- sexual history or sexual orientation
- adoption or surrogacy information

Permanence of the PII

The CMG assesses the relevancy and utility of the information over time and whether the information will permanently identify an individual. Some information loses its relevancy as it ages, while other information is likely to apply to an individual throughout their life. For example, an individual’s health insurance identification (ID) number can change but an individual’s health, such as family health history or chronic illness, may remain relevant for an individual's entire life, as well as the lives of their family members.

Number of Individuals Affected

The CMG will consider the number of affected individuals when determining the method(s) for providing notification. The CMG will also consider whether the breach may impact some affected individuals more than others. For example, if the breach includes information with a greater potential of harm for only a subset of individual, notification may be appropriate for only that subset.

Note: In some cases, the CMG may know who received/discovered the compromised PII. Many times, a breach is often reported by the recipient who received the information in error. This information, when available, may assist the NRC assess the likelihood of harm to impacted individuals.

- For instance, when an NRC employee inadvertently sends an individual's PII via email to another NRC employee who does not have a need to know, it may be reasonable to conclude that the risk of harm is low enough that the response may not necessitate a notification to the affected individual whose PII was compromised.

Likelihood of Access or Use of the Information

The NRC will consider the security safeguards, format and media, publicly available versus internal only, whether the breach was intentional or unintentional, evidence of misuse, and the duration of exposure when determining the likelihood that PII will be or has been used by unauthorized individuals.

- Electronic Security Safeguards such as encryption, data masking, or physical security safeguards that may still have been in place despite the breach. These are examples that will reduce the risk of harm.
- Format of PII or the media it is maintained on will affect the likelihood of access. For example, a spreadsheet on a portable USB drive does not require any special skill or knowledge to access compared to an encrypted removable hard drive which would require special expertise or knowledge of the password to access the information.
- The duration of exposure plays a key role in assessing the likelihood of access and use. PII that was exposed for an extended period of time is more likely to have been accessed or used by unauthorized individuals.
- Whether the breach was intentional or unintentional, or whether the intent is unknown.
- Evidence of misuse, including any evidence confirming that the PII was misused or that it was never accessed.
- Data publicly available or internal to NRC staff only.

Other considerations might include the likelihood that an unauthorized individual will know the value of the information and either use the information or sell it to others. In assessing the levels of risk and harm, the NRC will consider all element(s) and the broad range of potential harm flowing from their disclosure to unauthorized individuals.

5 Determining the Risk Rating of a Breach

When determining the risk rating, the NRC assesses the likelihood the incident may impact (cause harm) to affected individuals.

The level of harm that could occur is based on the method of data loss, type of data involved, ability to access the data, ability to mitigate the risk of harm, and the evidence of misuse in the actual breach in combination with the factors surrounding the breach as defined in Section 4 of this document.

The possible data elements and details surrounding the breach are listed in the tables below to assist the NRC in determining the likelihood of a confirmed breach causing harm to individuals and to what magnitude. These tables also appear in the CMG Report Template where the specifics for the breach would be noted along with the recommended risk rating.

5.1 Overall Likelihood of Harm Occurring

Data loss occurs when data is destroyed, corrupted, stolen, or made unreadable by software applications and users. It can be accidental (human error) or intentional.

Table 5.1-1: Method of Data Loss

Factor	Method of Data Loss	Selected Rating (H, M, L)
High	Online system hacked	
High	Data were targeted	
Moderate	Device was targeted	
Moderate	Device stolen	
Low	Device lost	
Low	Inadvertent release/spill	

Certain data elements are particularly sensitive and may alone present an increased risk of harm to the individual. The NRC evaluates the sensitivity of PII data and how easily the PII can be used to identify individuals, including the permanence of the PII (i.e., how long it will be relevant to the individual and whether it can be easily replaced or substituted). In addition, the NRC evaluates the extent to which the PII contains information that an individual would generally keep private. Such "private information" may not present a risk of identity theft or other criminal conduct but may pose a risk of harm such as embarrassment, blackmail, or emotional distress. The NRC also evaluates the context in which the data is used, as data elements that may otherwise present low or moderate risk could warrant a higher risk rating if justified by the context in which the data appears.

Table 5.1-2: Type of Data Elements Breached

Factor	Type of Data Elements Breached	Selected Rating (H, M, L)
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	Derogatory personnel or criminal information causing embarrassment (e.g., DUI, arrest)	
Moderate	The meaning of the data to the individual and the implications of exposure (e.g., Protective Job Series, investigators)	
Moderate	Date of Birth	
Moderate	Government-issued identification number (e.g., driver’s license)	

Table 5.1-2: Type of Data Elements Breached

Factor	Type of Data Elements Breached	Selected Rating (H, M, L)
Low	Name	
Low	Address – email address	
Low	Telephone number	
Other	Specify Details -	

Data access is the ability to retrieve, modify, copy, or move data. Access control is a data security process that enables individuals to manage who is authorized to access data. NRC evaluates the method the data was released to an unauthorized person.

Table 5.1-3: Ability to Access Data

Factor	Ability To Access Data	Selected Rating (H, M, L)
High	Data released publicly (i.e., public ADAMS)	
High	Electronic records that were not encrypted (i.e., outgoing email)	
High	Data stored externally without proper access controls (i.e., cloud service provider or contractor site)	
Moderate	Data stored Internally without proper access controls (i.e., Share Point)	
Moderate	Paper records left unprotected (i.e., plain sight)	
Low	Data only accessible internally (i.e., NRC Staff or contractors)	
Other	Specify details:	

Risk mitigation is the practice of reducing the negative effects of a breach. NRC evaluates the mitigation efforts that have taken place since the breach was discovered.

Table 5.1-4: Ability to Mitigate Risk of Harm

Factor	Ability to Mitigate Risk of Harm	Selected Rating (H, M, L)
High	No recovery of device or data	
High	Recovery of device or data, but high likelihood that data was accessed	
Moderate	Partial recovery of device or data	
Moderate	Recovery of device or data, but moderate likelihood that data was accessed	
Low	Recovery of device or data before use	
Low	Recovery of device or data, but low likelihood that data was accessed	
Other	Specify details:	
A description of any mitigation steps taken is provided below:		

The NRC will consider the security safeguards, format/media, publicly available versus internal only, and the duration of exposure when determining the likelihood that PII will be or has been misused by unauthorized individuals. The NRC will also consider whether the recipient of the PII disclosure (if not the general public) is known or unknown, and if the recipient is known, the trustworthiness of the recipient. Note that the descriptions below are intended to cover a range of potential scenarios and the risk ratings that would likely apply to each. Determining risk as it relates to evidence of malicious purposes can be very dependent on the specific circumstances of the breach, it is intended to be illustrative, not exhaustive or conclusive.

Table 5.1-5: Evidence of Data Used for Malicious Purposes

Factor	Evidence of data used for malicious purposes	Selected Rating (H, M, L)
High	• PII Data (electronic or hard copy) publicly available and either (1) cannot be removed from the public domain, or (2) no log data is available to determine if information was accessed while publicly available and the information was publicly available for a significant length of time or (3) log data is available and indicates improper access occurred, or (4) paper documents exposed to the public, left unattended or incorrectly disposed of. • Data was not available to the general public, evidence was found suggesting that PII data was or will be misused, including evidence indicating likely malicious intent by any unauthorized persons who were known or suspected to have accessed or received the PII.	
Moderate	• PII Data publicly available but has been removed from public domain and log evidence is available and appears consistent with a limited likelihood of misuse, or • The PII data was publicly available for only a short period of time and then removed and no evidence was found indicating the information was accessed with malicious intent or by a significant number of persons during the limited period of public availability, or • PII data was available only to a limited set of known individuals whose trustworthiness is uncertain (i.e., no strong evidence of either trustworthiness or untrustworthiness).	
Low	• PII data was publicly available, but has since been removed, and log evidence indicates that the data was not accessed by any unauthorized persons, or • PII was not publicly available, and evidence indicates that improper access, if any, was limited to individuals considered trustworthy and under circumstances that do not suggest malicious intent.	

The table below provides the descriptions for the three risk ratings when determining the likelihood based on available evidence.

Table 5.1 6: Risk Ratings to Determine Likelihood

Likelihood	Definition
High (H)	The nature of the breach and the data gathered during the investigation indicate that it is highly likely to have an adverse impact on the individual(s).
Moderate (M)	The nature of the breach and the data gathered during the investigation indicate that it is somewhat likely to have an adverse impact on the individual(s).
Low (L)	The nature of the breach and the data gathered during the investigation indicate that it is unlikely to have an adverse impact on the individual(s).

The table below provides the overall likelihood rating using each of the five key elements.

Table 5.1 7: Overall Likelihood Rating
(Information from Tables 5.1-1 – 5.1-5)

Description	Method of Data Loss Table 5.1-1	Type of Data Elements Breached Table 5.1-2	Ability to Access Data Table 5.1-3	Ability To Mitigate Risk of Harm Table 5.1-4	Evidence of Data Use for Malicious Purposes Table 5.1-5	Overall Likelihood
Rating						

5.2 Determining Impact/Harm

The NRC considers what the degree of impact to the individual could be if harm does, in fact, occur.

The NRC would consider the potential for harms such as identity theft, embarrassment, inconvenience, potential for blackmail, unfairness, harm to reputation, or the potential for harassment or prejudice, particularly when the breach involves information about health or financial benefits information. In doing so, the NRC would also consider the extent to which the breached information identifies or disproportionately impacts a particularly vulnerable population.

Table 5.2-1: Impact/Harm Assessment Scale

Impact Rating	Description	Selected Rating (H, M, L)
High	Event might result in severe or catastrophic harm, embarrassment, inconvenience, or unfairness to any individual on whom information was disclosed.	
Moderate	Event might result in significant harm, embarrassment, inconvenience, or unfairness to any individual on who information was disclosed.	
Low	Event might result in limited or no harm, embarrassment, inconvenience, or unfairness to any individual on whom information was disclosed.	

5.3 Summarizing the Overall Risk

Using Table 5.3-1, the CMG assigns an overall risk (combination of likelihood and impact/harm).

Table 5.3-1: Determining Overall Risk

Likelihood	Impact			Overall Risk Rating
	Low	Moderate	High	
High	Moderate	High	High	
Moderate	Low	Moderate	High	
Low	Low	Low	Moderate	

Once the overall risk is determined, the corresponding action is assigned.

Table 5.3-2 summarizes the overall actions that will be taken.

Table 5.3-2: Overall Actions

Risk Score	Necessary Action	Selected
High	Notify and provide credit monitoring	
Moderate	Notify only	
Low	Monitor only - breach report sent to SAOP-not to CMG	

6 Submitting Risk Determination to the CMG

At the conclusion of the risk analysis process, the SAOP provides the draft CMG Report summarizing the facts surrounding the breach with the recommended responses for their **consideration and concurrence** for those resulting in a Moderate or High-Risk rating. The CMG assesses the likelihood, impact level, and risk of potential harm that could occur and ensures that appropriate steps are initiated to mitigate the breach's impact and recurrence, in compliance with Federal guidance.

A breach notification is provided to the affected individuals when the risk rating is Moderate or High, but **not for a Low-risk rating**. If the response can be conducted at the staff level, the NRC will not assemble the CMG.

If the risk factors are not identical within a group of affected individuals, then notification may be appropriate for a subset of the group. Therefore, consideration should be given to all elements when determining final actions to be taken when addressing each incident. In circumstances where a breach notification could increase a risk of harm, the CMG may decide to delay a notification until appropriate safeguards are put in place.

For those breaches resulting in a Moderate or High-risk ratings, the SAOP notifies the NRC office responsible for the incident, which may include:

- individual(s) being notified
- providing credit monitoring services
- recommending disciplinary measures depending on the situation

7 Notification Process

When it has been determined that a breach notification is appropriate, 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 or to allow the time 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 notification is required regarding the breach. However, the CMG will not allow any delay that will exacerbate risk or harm to any affected individuals.

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

The CMG will determine the appropriate composition of the audience to receive the 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.

7.1 Traditional Means of Providing Notifications

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 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 utilize the following means of notification:

Telephone

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

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. The notice should be sent separately from any other mailing. If another agency is used to facilitate mailing, 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.

Email

Email notification can be problematic because individuals change their email addresses and may not notify third parties of the change. While notification by postal mail is preferable, notification by email might be appropriate if an individual has provided an email address to the NRC and has expressly given consent to use email as the primary means of communication with the NRC, and no known mailing address is available. Email notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. Email notification may include links to the NRC's public Website 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 Website is appropriate.

7.2 Supplemental Means of Providing Notifications

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 Website and a 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 check to see if their personal information is included in the breach.

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 actions, including the notice, have 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.

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 Website as soon as possible. The posting should include a link to frequently asked questions (FAQs) and other information to assist the public's understanding of the breach and the notification process.

Other Public and Private Sector Agencies

The CMG will determine whether other public and private sector agencies should be notified particularly those that might be affected by the breach or might play a role in mitigating the potential harm stemming from the breach. The NRC may use Government-wide services already in place to provide support services.

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.

Note: 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 Website.

7.3 Contents of Breach Notice

The agency will provide notification in writing using concise, plain language. The notice will include the elements provided in Table 7.3-1, as applicable.

Table 7.3-1: Breach Notification Requirements

Elements required	Examples
A brief description of what happened	Include the date(s) of the breach and the date of its discovery
A description of the types of PII, but not the specific PII involved in the breach	Information such as full name, SSN, date of birth, home address, or account number would not be provided in the notification
Indicate if the information was encrypted or protected by other means	Describe how information was encrypted or other methods of protection, if applicable
Steps an individual should take to protect themselves	Include suggested actions such as: • Credit and identity monitoring services • Free credit reports • Contact Federal Trade Commission for more credit protections including fraud alert information
Steps the NRC is taking to investigate the breach	Describe steps taken to mitigate losses and protect against similar or additional breaches
Provide agency contacts for more information	Office Director responsible must provide an email address and phone number to field questions for those individuals impacted by the spill
If a breach includes financial information	Individual should contact financial institution(s) to determine whether the account(s) should be closed
If the breach includes information that can be used to open a new credit account	• Include how to request a free credit report • Contact financial institution to place an initial fraud alert on credit report • Monitor their financial account statements and immediately report any suspicious or unusual activity to the responsible financial institution • A recommendation that the individual consider placing a credit freeze on their 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)

8 Infractions That May Impose Disciplinary Measures

In accordance with the existing authority, the NRC may impose progressive disciplinary measures on employees and/or contractors for infractions of agency PII policy.

The following infractions may constitute a basis for disciplinary measures, including reprimand, suspension, removal, or other actions consistent with applicable law and policy:

Lack of PII Security Controls

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

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.

Unauthorized Access

Deliberate unauthorized access to or solicitation of PII may constitute a basis for disciplinary measures. 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.

Failure to Report

Failure to report any known or suspected loss of control or unauthorized disclosure of PII may constitute a basis for disciplinary measures.

Supervision and Training

OCIO trains 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 "Cybersecurity Security Awareness Training" and "Personally Identifiable Information (PII) & Privacy Act Responsibilities Awareness" required training. Failure, as a supervisor, to adequately instruct, train, or supervise employees in their responsibilities may constitute a basis for disciplinary action.

9 References

9.1 Federal Laws

- Federal Information Security Modernization Act (FISMA) of 2014, Pub. L. 113-283, 128 Stat. 3073 (Dec. 18, 2014) (primarily codified at 44 U.S.C. chapter 35, subchapter II). Available at: https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf
- 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

9.2 Memoranda, Special Publications, Executive Orders and Directives

- OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information (Jan. 3, 2017). Available at: https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12_0.pdf

- OMB Memorandum M-19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program (Dec. 10, 2018). Available at: https://www.whitehouse.gov/wp-content/uploads/2018/12/M-19-03.pdf

  OMB Memorandum M-20-04, Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements (Nov. 19, 2019). Available at: https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf

- PPD-41, Annex for Presidential Policy Directive – United States Cyber Incident Coordination (July 26, 2016). Available at: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/annex-presidential-policy-directive-united-states-cyber-incident

- OMB Memorandum M-16-14, Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response (July 1, 2016). Available at: https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2016/m-16-14.pdf

- NIST Special Publication 800-122, Guide to Protecting the Confidentiality of PII (Apr. 2010).

- Federal Incident Notification Guidelines

9.3 NRC Policy

- U.S. Nuclear Regulatory Commission, “Privacy Act,” MD 3.2, as amended
- U.S. Nuclear Regulatory Commission, “NRC Cybersecurity Program,” MD 12.5, as amended
- U.S. Nuclear Regulatory Commission, “Privacy Program Plan”

10 Appendix A: Flow Chart of the Breach Notification Process