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

Office of the Chief Information Officer (OCIO)

Version 2.1

February 29, 2024

Document Revision History

Date	Version	Description	Author
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 privacy breach, as defined by 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 ➢ Determines if a breach notification is required along with the appropriate actions

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
Network and Security Operations Branch 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 NSOB 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)	➢ Responsible for funding the credit monitoring service
Office of the Chief Information Officer (OCIO) Division of Resource Management and Administration (DRMA)	➢ Administers the credit monitoring contract ➢ DRMA engages the contractor to set up credit monitoring services ➢ DRMA provides necessary enrollment instructions for credit monitoring services for those impacted by the breach

3 Reporting of Suspected or Actual Breach of PII

It is NRC policy that all NRC staff and contractors immediately 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-23-03, *Fiscal Year 2023 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 Determining if a Breach Notification is Required

To determine whether a breach notification is required, 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; **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.

Rating	Notification Action
High	Notify and provide credit monitoring
Moderate	Notify only
Low	Monitor only - breach report sent to SAOP-not to CMG

***Note**:* Appendix A details the steps involved in determining the overall level of risk rating and associated actions.

4.1 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 to provide notice 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 program 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.

4.2 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.

4.3 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**.**

4.4 Contents of Breach Notice

The agency will provide notification in writing using concise, plain language. The notice will include the elements provided in Table 4.4-1, as applicable:

Table 4.4-1: 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	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)

5 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.

6 References

6.1 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

6.2 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).

6.3 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

7 Analyzing the Risk of a Breach

Determining risk is a combination of analyzing the likelihood of exploiting a privacy violation and the resulting impact of that violation. The CMG will review the draft risk analysis and provide concurrence and/or other recommendations to the SAOP for final approval. Upon final approval, the NRC Privacy Officer will finalize the risk analysis report.

The SAOP notifies the NRC office responsible for the incident, including:

- Can the risk be mitigated?
- Should the individual(s) be notified?

- Should credit monitoring be offered?
- Should management consider taking appropriate disciplinary measures against the person(s) responsible for the breach?

In determining the likely risk of harm and level of impact, the CMG considers the factors below to determine when, what, how, and to whom a breach notification should be given.

Nature of the Breach

- Was the LAN/WAN, or other applications/data store systems accessed?
- Is there any evidence of harm because of the breach?
- What vulnerability was exploited?
- What actions can or should be taken before, or in conjunction with, notification?

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
- 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 context of the data element(s) and the broad range of potential harm flowing from their disclosure to unauthorized individuals. If the data elements include financial information and it was determined that the NRC was responsible for the breach, the NRC will provide credit monitoring services.

Number of Individuals Affected

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 decides to provide a 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.

Likelihood That the 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 would influence the CMG's decision regarding whether to provide a 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, depending

on whether any physical, technological, or procedural safeguards have been applied to protect the information.

Not all encryption is created equal. If the information is properly protected by encryption, or special software is required to read or access the data, the risk of compromise must be evaluated.

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.

7.1 Determining the Likelihood of an Incident

To assess the overall likelihood of a breach occurring, the CMG considers the following five key elements:

1. Method of Data Loss
2. Type of Data Elements Breached
3. Ability to Access Data
4. Ability to Mitigate the Risk of Harm
5. Evidence of Data Used for Malicious Purpose

Table 7.1-1: 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	

Table 7.1-2: 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	

Factor	Type of Data Elements Breached	Selected Rating (H, M, L)
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 – email address	
Low	Telephone number	

Note: A combination of identifying information and financial or security information is always HIGH and a HIGH likelihood of harm occurring.

Table 7.1-3: Ability to Access Data

Factor	Ability To Access Data	Selected Rating (H, M, L)
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 (e.g., 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	

Table 7.1-4: Ability to Mitigate Risk of Harm

Factor	Ability to Mitigate Risk of Harm	Selected Rating (H, M, L)
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	
A description of any mitigation steps taken is provided below:		

Table 7.1-5: Evidence of Data Used for Malicious Purposes

Factor	Evidence of data used for malicious purposes	Selected Rating (H, M, L)
High	Data was published on the Web	
Moderate	Data accessed but no evidence of use	
Low	No evidence that data was accessed or used	

Table 7.1-6 provides the descriptions for the three risk ratings when determining the likelihood based on available evidence.

Table 7.1-6: Risk Ratings to Determine Likelihood

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.
Moderate (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.

Table 7.1-7 provides the overall likelihood rating using each of the five key elements.

Table 7.1-7: Overall Likelihood

Description	Method of Data Loss Table 7.1	Type of Data Elements Breached Table 7.2	Ability to Access Data Table 7.3	Ability To Mitigate Risk of Harm Table 7.4	Evidence of Data Use for Malicious Purposes Table 7.5	Overall Likelihood
Rating						

7.2 Determining Impact/Harm

After evaluating each of the five key elements and assigning an overall likelihood of a breach occurring, the CMG will review and assess the impact/harm to an individual or to the NRC.

Table 7.2-1 provides the descriptions for the three (3) impact/harm values to assist in determining the overall risk.

Table 7.2-1: Impact/Harm Assessment Scale

Impact Rating	Description	Selected Rating (H, M, L)
High	Event might: • result in human death or serious injury or harm to the individual; • result in high costs to the organization; or • significantly violate, harm, or impede the organization's mission, reputation, or interest.	
Moderate	Event might: • result in injury or harm to the individual: • result in costs to the organization; or • violates, harms, or impedes the organization's mission, reputation, or interest.	
Low	Event might: • result in the loss of some tangible organizational assets or resources; or • 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)).

7.3 Summarizing the Overall Risk

Using Table 7.3-1, the CMG assigns an overall risk (combination of likelihood and impact/harm).

Table 7.3-1: Determining Overall Risk

Likelihood	Impact			Overall Risk Level
	Low	Moderate	High	
High	Moderate	High	High	
Moderate	Low	Moderate	High	
Low	Low	Low	Moderate	

The CMG will assess whether the PII breach is at a low, moderate, or high risk of being compromised. Once the overall risk is determined, the corresponding action is assigned.

Table 7.3-2 summarizes the overall actions that will be taken.

Table 7.3-2: Overall Actions

Risk Score	Necessary Action	Selected
High	Notify and provide credit monitoring	
Moderate	Notify only	
Low	Monitor only	

This page intentionally left blank.

8 Appendix A: Flow Chart of the Breach Notification Process