United States Environmental Protection Agency (EPA)

Personally Identifiable Information (PII) Incident Handling & Response Procedure - CIO 2151-P-06

Version 1.2: January 31, 2008
Presented by: Office of Information Collection (OIC)

Overview

Background

In accordance with United States Code 552a (e) (10) Federal Agencies are required to *"establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained".* Recent recommendations and mandates such as the President's Identity Theft Task Forces' Memorandum entitled *Identity Theft Related Data Security Breach Notification Guidance* dated September 19, 2006 and the Office of Management and Budget (OMB) Memorandum M-07-16 entitled *Safeguarding Against and Responding to the Breach of Personally Identifiable Information (PII[1])* dated May 22, 2007 require each Agency to develop a procedure for handling and responding to PII incidents. Additional guidance is provided by the National Institute of Standards and Technology Special Publication 800-61 (NIST SP 800-61) entitled *Computer Security Incident Handling Guide* dated January 2004 for how the Federal Government should manage all information incidents.

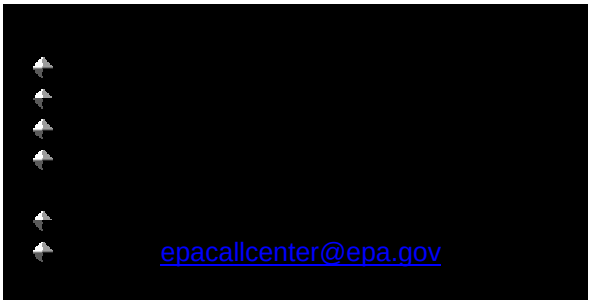
Purpose

This procedure seeks to assist Environmental Protection Agency (EPA) Officials in conducting their duties in the event of a PII incident by providing practical guidance on responding to incidents effectively and efficiently via the use of a incident taxonomy. The context of each incident may deviate from the examples provided in this text. Therefore, it may be required to tailor the handling and response activities to meet the specific security or business requirement presented.

Computer Security Incident Response Capability (CSIRC)

As referenced in the Agency's Breach of Personally Identifiable Information (PII) Notification Response Plan, the CSIRC is responsible for handling and response for all computer security incidents and reporting those incidents to the United States Computer Emergency Response Team (US-CERT). More explicitly and in accordance with OMB M-06-19 *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments* dated July 12, 2006; all incidents related to PII must be reported to US-CERT within one hour of discovery.

Therefore, all incidents to include, but not limited to, PII incidents must be reported to the EPA Call Center. While it is preferred the calls are reported by the appropriate local Information Security Officer (ISO) it is acceptable for users to report directly to the call center as well. Once the call center has received the call and conducts the initial triage, they will forward the call to the CSIRC. It is important to note that all PII incidents confirmed or suspected must be reported to the call center immediately to ensure CSIRC can respond to US-CERT within one hour.



[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

PII Incident Defined
A PII incident includes, but is not limited to, the unintentional or intentional loss of information; or unauthorized access, acquisition, modification or disclosure of PII information whether physical or electronic.

Incident Response and Handling

Incident Response and Handling Phases

The incident handling and response process has several phases, from initial preparation through post-incident analysis. PII incidents are incorporated into the phases and activities as are other information security incidents.

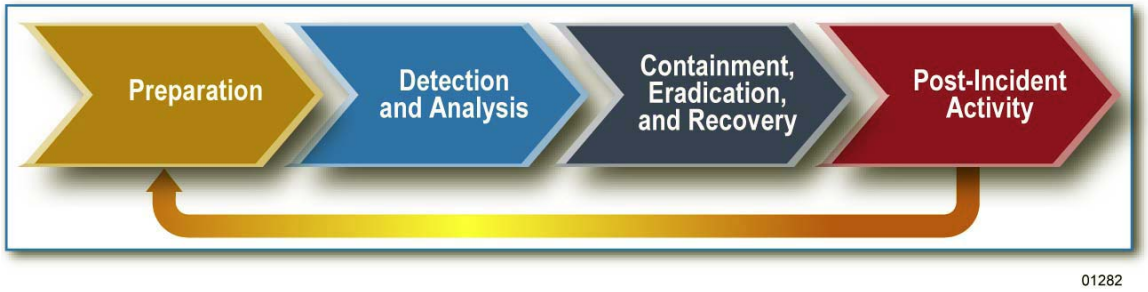


Figure #2 – Incident Response Life Cycle (NIST SP 800-61)

Preparation Phase

Preparation focuses primarily on identifying key resources for preventing and handling incident such as people, processes and tools. The existing CSIRC resource pool as identified in the Information Security Officer's (ISO) Handbook[2] is augmented by the following Agency's Breach of Personally Identifiable Information (PII) Notification Response Policy and Plan[3] entities:

- Senior Agency Office for Privacy (SAOP) or in Chief Information Officer (Assistant Administrator for the Office of Environmental Information)
- Breach Notification Team (BNT)
- Breach Evaluation Team (BET)

Detection and Analysis Phase

The first preparatory activity for a PII incident detection and analysis is to develop the PII incident taxonomy. Taxonomy is defined as the science of categorization, or classification, of things based on a predetermined system. In the case of PII incidents the predetermined "system" is category and severity level.

There are two types of categories of PII incidents that will be make up the first portion of the overall risk criteria:

- Category I –Sensitive (CAT I) – A CAT I incident is defined as a breach of sensitive PII. Sensitive PII is defined as Social Security numbers, or comparable identification numbers; financial information associated with individuals; and medical information

[2] Incident Response Handling/ISO Handbook http://intranet.epa.gov/otop/security/CSIRC/CSIRC_Handbook.pdf
[3] Breach of Personally Identifiable Information (PII) Notification Response Policy and Plan, location TBD

associated with individuals.[4]

- Category II –Non-Sensitive (CAT II) – A CAT II incident is defined as a breach of non-sensitive PII. Non-sensitive PII is defined all other PII not explicitly mentioned in the content and context of the Sensitive PII definition.

The severity of a PII incident is determined by the extent of the data breach in relation to disclosure vulnerability, and likelihood of PII data being exploited ~~successful occurrence~~. Each severity level is based on High, Moderate, and Low levels of severity on the individual and the organizations assets or operations. The severity levels are based on the following considerations;

Extent of Breach - Considerations

- Nature of the Data Elements Breached [Data and Context]
- Number of Individuals Affected

Consideration	Scenario
Nature of the Data Elements Breached	**A document, a set of documents or a database was lost or compromised containing social security numbers, credit card numbers and banking information, or medical information.**
Number of Individuals Affected	**The data set contains a substantial number (e.g. a least one hundred (100) or more individuals) or includes individual(s) that directly impact National Security or Continuity of Government (COG).**

Table #1H – Exploit Consideration Scenario – High

Consideration	Scenario
Nature of the Data Elements Breached	**A document, a set of documents or a database was lost or compromised containing PII apart from those elements identified in Table #1H that is not in the public domain.**
Number of Individuals Affected	**The data set contains a information on a moderate number of individuals (e.g., more than 10 but less than one hundred (100) individuals) or include information that could identify an individual(s) that directly impact National Security or Continuity of Government (COG).**

Table #1M – Exploit Consideration Scenario – Moderate

Consideration	Scenario
Nature of the Data Elements Breached	**A document, a set of documents or a database was lost or compromised containing PII that is in the public domain.**
Number of Individuals Affected	**The data set contains information or data on few individuals (e.g. less than 10) and does not include individual(s) that directly impact National Security or Continuity of Government (COG).**

Table #1L – Exploit Consideration Scenario – Low

Likelihood Considerations (Vulnerability-based)

- Likelihood the Information is Accessible and Usable
- Likelihood the Breach May Lead to Harm
- Ability of the Agency to Mitigate the Risk of Harm

[4] EPA Privacy Policy Sensitive PII Definition, http://www.epa.gov/privacy/policy/2151/index.htm

Consideration	Scenario
Likelihood the Information is Accessible and Usable	**Controls are not in place to adequately protect the data.** Example: The data in question is unencrypted, not adequately encrypted or encryption status is unknown. The printed information is loose (i.e., not enclosed in a sealed container) or the ease of its disclosure condition is unknown.
Likelihood the Breach May Lead to Harm	**The data compromised has the known or potential to link to an individual's specific financial or medical related information.**
Ability of the Agency to Mitigate the Risk of Harm	**The Agency is unable to contain, eradicate or recover.**

Table #2H – Likelihood Consideration Scenario – High

Consideration	Scenario
Likelihood the Information is Accessible and Usable	**Controls are not fully in place to adequately protect the data.** Example: The data in question is believed to be encrypted or adequately encrypted. Printed information has limited disclosure protection. Information was returned but evidence of tampering not conclusive or reliability of source not clear.
Likelihood the Breach May Lead to Harm	**The data compromised is limited linkage to an individual's specific financial or medical related information.**
Ability of the Agency to Mitigate the Risk of Harm	**The Agency is believed to be able to sufficiently contain, eradicate or recover.**

Table #2M – Likelihood Consideration Scenario – Moderate

Consideration	Scenario
Likelihood the Information is Accessible and Usable	**Controls are substantially in place to adequately protect the data.** Example: The data in question is encrypted or in a sealed container with the outer layer containing a postage paid return address. Information or lost device is returned in a timely manner with no identifiable disclosure or access. The information or device was in the safe keeping of a source believed to be reliable for all or most of the time it was missing or lost.
Likelihood the Breach May Lead to Harm	**The data compromised has no known potential to link an individual's to specific financial or medical related.**
Ability of the Agency to Mitigate the Risk of Harm	**The Agency is able to contain, eradicate or recover.**

Table #2L – Likelihood Consideration Scenario – Low

With these considerations in mind the first risk matrix is provided to guide the decision of overall likelihood of a PII incident:

Likelihood	Liklihood Definition
High	The security of the data and controls to minimize the likelihood of a privacy violation are **ineffective**.
Moderate	The security of the data and controls to minimize the likelihood of a privacy violation are **minimally effective**.
Low	The security of the data and controls to minimize the likelihood of a privacy violation are **substanially effective**.

Table #3– Risk Matrix - Likelihood Definitions

The severity of the PII incident is determined by the extent of the data breach and the a risk of harm to the individual(s) or the Agency. Therefore the following Severity Levels are provided to assess the level of severity.

- High – A High severity incident is a breach that would be extremely or Catastrophically adverse to the organizational operations, organizational assets or individuals. Examples include, but are not limited to, the incident (1) may result in human death or serious injury or harm to individual(s); (2) may result in high cost to the EPA or individuals; (3) is National or International in scope; or (4) may significantly violate, harm or impede EPA's mission, reputation, or interest.

- Moderate – A moderate severity incident is a breach that would be Seriously adverse to the organizational operations, organizational assets or individuals. Examples include, but are not limited to, the incident (1) may result in injury or harm to the individual; (2) may result in costs to EPA or individuals; (3) is Regional or Nationally limited in scope; or (4) may violate, harm, or impede EPA's mission, reputation or interest.

- Low – A Low severity incident is a breach that would be of Limited significance to organizational operations, organizational assets or individuals. Examples include, but are not limited to, the incident (1) may result in loss of some tangible EPA asset or resource; (2) costs are minor or insignificant; (3) is local or otherwise limited in scope; or (2) may noticeably affect EPA's mission, reputation, or interest.

Severity Level	Severity Level Definition
High	A SEV I is a breach that would be **Extremely** or **Catastrophicly adverse to** organizational operations, organizational assets or individuals.
Moderate	A SEV II is a breach that would be **Seriously adverse to** organizational operations, organizational assets or individuals.
Low	A SEV III is a breach that would be of **Limited significance to** organizational operations, organizational assets or individuals.

Table #4 Risk Matrix - Severity Definitions

The analysis of these factors (Extent of Breach, Vulnerability-based Likelihood and Severity Level) assists in the initial determination of risk of PII disclosure to the individual and EPA, and the selection of an overall severity level rating for the incident to arrive at a subsequent notification action.

Risk Score - Notification Criteria			
	SEVerity Level Designations		
Likelihood	Low	Medium	High
High	**SEV II - Medium**	**SEV I - High**	**SEV I - High**
Moderate	**SEV III - Low**	**SEV II - Medium**	**SEV I - High**
Low	**SEV III - Low**	**SEV III - Low**	**SEV II - Medium**

Table #5 Risk Criteria - Severity

The BET will assign a Category and Severity resulting in incident nomenclature such as CATI-SEVI for category level one (sensitive PII) / severity level I. This accumulative score is known as the Risk Score.

Containment, Eradication & Recovery Phase

During the standard containment, eradication and recovery activities conducted by the CSIRC or Privacy office as identified in NIST SP 800-61, *Computer Security Incident Handling Guide*, the BRT's activities will focused on the execution of appropriate notification procedures.

Standard notification procedures are assigned to each CAT/SEV based Risk Score. In accordance with OMB M-07-16[5], each of these procedures will take into consideration the following:

- Timeliness of the Notification
- Source of the Notification
- Contents of the Notification
- Means of Providing Notification
- Recipients of the Notification

For all CAT I PII incidents the following notification actions are required:

Risk Score	Notification Actions
SEV I (High)	Notify within 48 hours of Risk Evaluation and provide support services. Make extensive efforts to notify all impacted individuals.
SEV II (Moderate)	Notify within 48 hours to 5 business days of Risk Evaluation, provide support services upon request.
SEV III (Low)	No Notification - Monitor.

Table #6 Notification Actions

Timeliness of the Notification

As previously indicated, all notification for Category I PII incident should take place within (48) business hours of the completion of the risk evaluation and score determination. The time between discovery and reporting is one (1) hour. The time between reporting and risk evaluation should not exceed (48) hours. All Category II PII incident notifications should take place with a reasonable time following the risk evaluation and score determination; not to exceed five (5) business days.

Each Category within its provided constraints should also consider legitimate time requirements of law enforcement and national security entities. Such examples include the need for delays in notification if the investigation of the incident would result in seriously impeding the progress or success of the investigative activities. It is important to the note that the delay should not exacerbate risk or harm to the individual, Agency or related investigations.

Source of the Notification

All notifications are required to come from EPA's will ensure that all internal and external interdependencies have been taken into considerations to ensure the containment of the incident's impact.

Contents of the Notification

In accordance with OMB M-07-16, the notification will include the following elements:

- A brief description of what happened, including the date(s) of the incident and of its discovery;
- A description of the types of personal information involved in the incident;
- A statement whether the information was appropriately protected, when determined such information would be beneficial and would not compromise the security of the system or the EPA;
- What steps individuals should take to protect themselves from potential harm, if any;
- What the EPA is doing to investigate the incident, to mitigate losses, and to protect against any further breaches; and

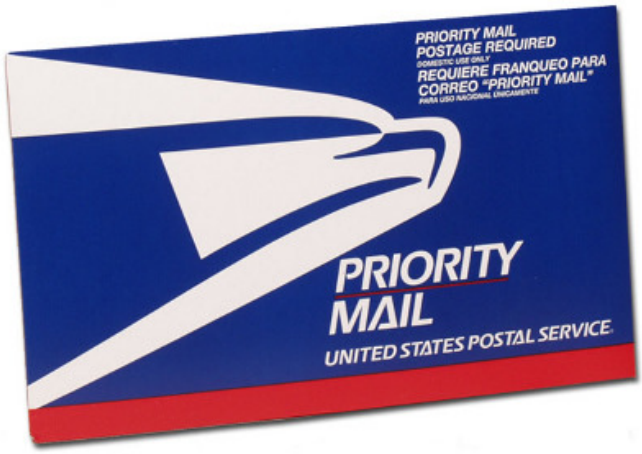
[5] OMB M-07-16, *Safeguarding Against and Responding to the Brach of Personally Identifiable Information*

- Who affected individuals should contact at the EPA for more information, including a toll-free telephone number, e-mail address and postal address.

Target Audience & Means of Providing Notification

Notice of the incident will be provided commensurate to the number of individuals affected and the availability of contact information. Correspondence will be prominently marked on the exterior reflecting the importance of the communication to ensure the recipient does not discard or otherwise ignore the notification.

The Primary means of notification will be by first-class or priority mail to the last known mailing address of the individual based on EPA's records. Where EPA has reason to believe the address is no longer current, reasonable efforts will be made to update the address using the U.S. Postal Service National Change of Address (NCOA) database.



Substitute notices may be made in instances where EPA does not have sufficient contact information for those who need to be notified. In such instances, notice may consist of a conspicuous posting of the notices on the EPA web site home page and home page including additional information in a Frequently Asked Questions (FAQ).

Notification may be provided to major print and broadcast media in areas where the affected individuals reside. Additionally, the notice to media will include a toll-free phone number where an individual can learn whether his or her personal information was included in the breach.

Appropriate consideration will be made for information where the source is a partner Federal Government Agency thus ensuring appropriate Memorandum's of Agreement/Understanding have been met. Private Sector Agencies, in accordance with appropriate contracts, will also receive specific consideration for notification.

Special consideration will be given in providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Action of 1973. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the EPA web site.

In the event of a Congressional Inquiry the EPA Office of Congressional Affairs will provide the appropriate initial notification and subordinate response in coordination with appropriate internal organizations.

Support Services

CAT I/SEV I incident will provide additional support services to individual such as credit monitoring. EPA will use the General Services Administration (GSA) Blanket Purchase Agreement (BPA) 10266 for these services to eliminate potential delays associated with contracting and open market cost.[6]

- GS-23F-06-E3-A-00013 Bearak Reports (Woman-Owned, Small Business)
- GS-23F-06-E3-A-00014 Equifax Inc. (Large)

[6] OMB M-07-04, *Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)*

- GS-23F-06-E3-A-00015 Experian Consumer Direct (Large)

Post-Incident Activity Phase

Each incident will close with a formal Lessons Learned to measure effective and ineffective activities during the incident. These lessons will be utilized to enhance the existing policy, procedures and training.

Additionally, all artifacts associated with the PII brief will be maintained by the Privacy Office. This includes, but is not limited to, artifacts developed by Public Affairs, Congressional Affairs and CSIRC.