

United States Environmental Protection Agency
Breach of Personally Identifiable Information (PII) Notification
Response Procedures

Revised: January 14, 2008

I. Introduction and Overview

The Environmental Protection Agency (EPA) developed this Breach Notification Response Procedures (hereafter referred to as "Procedures") in response to memoranda that the Office of Management and Budget (OMB) issued to federal agencies in (1) 2006 and 2007 and in furtherance of its responsibility and commitment to adequately safeguard all personally identifiable information (PII) in its possession.

The OMB memoranda require each agency to develop and implement a procedure for responding to data breaches and to establish a core management group to respond to the loss of PII should such a data breach occur. OMB recommends that the core group include, at minimum, the agency's chief information officer, chief legal officer, inspector general, and other senior management officials (or their designees). The core group ensures that the agency has brought together staff with expertise in information technology, legal authorities, and law enforcement necessary to respond to a data breach. This Procedure 1) identifies the Agency's senior management officials who comprise the core management group (i.e., the Breach Response Team, or BRT); 2) identifies the first-level review and analysis team (i.e., the Breach Evaluation Team (BET)); 3) outlines the process the Agency will follow to handle breaches of PII and incidents posing a potential risk of identity theft; and 4) identifies roles and responsibilities of response teams and key Agency offices that will likely be involved in breach mitigation and notification activities.

The EPA Administrator has delegated to the Chief Information Officer (CIO), currently the Assistant Administrator for the Office of Environmental Information (OEI), the responsibility to ensure the Agency's implementation of protections for privacy information. The CIO is also the Senior Agency Official for Privacy (SAOP).

¹ OMB Memorandum regarding "Recommendations for Identity Theft Related Data Breach Notification," issued on September 20, 2006. The 2006 OMB memorandum also is available at (http://www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

OMB Memorandum (M-07-16) regarding "Safeguarding Against and responding to the Breach of Personally Identifiable Information," issued on May 22, 2007. The 2007 OMB memorandum also is available at <http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf>. [this link is not hot]

This procedure sets out processes that supplement current Agency procedures for protecting PII, incident handling and notification and federal requirements for reporting and handling incidents pursuant to the Agency's Privacy Policy, Federal Information Security Management Act of 2002 (FISMA), National Institute of Standards and Technology Special Publications (NIST) Special Publication 800-61, Computer Security Incident Handling Guide, and the concept of operations for United States Computer Emergency Readiness Team (US-CERT) The Office of Technology and Operations Planning (OTOP) and the Office of Information Collection (OIC) are responsible for ensuring compliance with policies and procedures as set forth in this paragraph. Criminal violations are determined and investigated by the Office of the Inspector General, Office of Investigations (OIG/OI).

The audience for this procedure includes all parties involved in its implementation and those parties who may need to respond to a known or suspected breach. (See Section IX of this document.)

II. Reporting Incidents

Pursuant to EPA's Privacy Policy, all Agency officials, staff, contractors and others working at the Agency are directed to immediately report any suspected or known breach of PII. Incidents must be reported to the primary Information Security Officers (ISO) and to the EPA Call Center at 1-866-411-4372 as soon as the breach or suspected breach is discovered.

A. The EPA Call Center

The EPA Call Center, managed by OEI, has established processes and procedures for reported issues or incidents. The initial contact with the caller will attempt to elicit as much information as possible, but follow-up or further investigation may be necessary to obtain sufficient data. The initial assessment by the Call Center will attempt to identify whether any PII is involved, and if so:

- Type of PII (sensitive or other);
- Date of incident;
- Nature of incident and the means by which the breach occurred;
- Unauthorized access to information;
- Unauthorized use of information;
- Where the information was stored;
- Name of the system/records;
- System or network intrusion;
- Loss of control of paper documents containing sensitive information;
- Person who reported incident, including contact information;

- Person who discovered incident, including contact information.
- Number of individuals potentially affected;
- Number of records potentially affected;
- Accessibility of the information; and
- Individual responsible for the incident.

If the information provided by the caller appears to involve PII, the Call Center will immediately transfer the incident report to the Agency's Computer Security Incident Response Capability (CSIRC) Team.

B. Computer Security Incident Response Capability (CSIRC) Team

CSIRC is responsible for handling computer security-related incidents and reporting of incidents internally and to the United States Computer Emergency Readiness Team (US-CERT) at the Department of Homeland Security. CSIRC will work with the Information Security Officer (ISO) of the affected organization and others, as appropriate, to investigate the incident when reported by the Call Center. The ISO will coordinate with the appropriate Liaison Privacy Official, as appropriate. Any information not available or elicited from the caller by the Call Center will be obtained by CSIRC and recorded in the incident report database. If the breach is believed to involve a possible criminal violation, CSIRC will immediately notify the OIG/OI. CSIRC will complete its investigations as quickly as possible and report its findings to the Breach Evaluation Team.

C. Report of PII Incident Findings

Breach Evaluation Team (BET)

CSIRC will report its findings to the Director, Technology and Information Security Staff, OTOP who will co-chair the BET with the Chief, Records, FOIA and Privacy Branch. The co-chairs and their senior staff will review the CSIRC report, identify whether additional information is needed to evaluate the risk, conduct a risk analysis of the breach using the Agency's "PII Incident Handling & Response procedures" and decide whether to recommend convening the core management group, i.e., the Breach Notification Team, along with recommendations for the Agency's next steps for addressing the findings.

In considering the likely risk of harm caused by the known or suspected breach, the BET will use a risk-based categorization that considers the accessibility of the breached information (e.g., whether the information is encrypted) along with other factors and a wide range of potential harms to both the Agency and the affected individuals as identified in OMB's memorandum M-07-16. As prescribed by OMB, the BET will consider risk of identify theft, harm to reputation, criminal violation

possibilities, embarrassment, inconvenience, unfairness, harassment, and prejudice, particularly when health or financial information is involved in the breach.

United States Computer Emergency Readiness Team (US-CERT)

In accordance with OMB M-06-19, "*Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*", CSIRC will report all PII-related incidents to US-CERT within one hour of discovery.

III. Review by the Breach Response Team (BRT)

The Senior Agency Official for Privacy (SAOP) will convene the BRT, if appropriate, to determine the Agency's next steps.

The BRT will review the investigatory findings, the analysis of the likelihood of risk to affected individuals and to the Agency and make final decisions regarding the Agency's response to the known or suspected breach.

A. Responding to the Breach

If the BRT determines there is a risk of identity theft from a breach of PII or that there is a risk of likely harm to the affected individuals other than the risk of identify theft, it will determine the course of action. In developing the course of action to address the breach, the BRT will consider the options available to agencies and individuals to protect potential victims of identity theft as set forth in OMB memorandum M-07-16, dated May 22, 2007).

In summary, for individuals these include:

- Contacting financial institutions;
- Monitoring financial account activity;
- Requesting a free credit report;
- Placing an initial fraud alert on credit reports;
- For residents of states in which it is authorized under state law, considering placing a freeze on their credit file;
- Reviewing resources at www.idtheft.gov.

For agencies, these include:

- Engaging a third party to conduct a data breach analysis to determine whether a particular data loss appears to be resulting in identity theft; or

- Providing credit monitoring services if the BRT has determined that such services are required to mitigate potential damage due to the breach.

B. Taking Steps to Contain and Control the Breach

The BRT will coordinate with other EPA offices, as needed, to ensure that appropriate steps are taken to contain and control the breach and to determine what safeguards need to be put in place to keep such a breach from re-occurring.

IV. Incidents Involving Breaches of Electronic and Paper PII

The SAOP, in coordination with the BRT members, including the Office where the breach occurred, will take all necessary steps to contain, control and mitigate the risks from the breach and prevent further unauthorized access to or use of individual's information, including: (1) monitoring, and possibly freezing, or closing affected accounts; (2) modifying computer access codes or physical access controls; and (3) taking other necessary and appropriate action having consulted with the OIG/OI. The SAOP will take these steps without undue delay and consistent with current requirements under the Federal Information Security Management Act (FISMA) and Agency policies.

V. Incidents Involving Breaches of Physical Security

If the breach involves physical security incidents that affect privacy, the EPA Security Staff in OARM shall ensure that necessary steps are taken to contain and control the breach and prevent further unauthorized access. Such steps may include changing locks or key codes, deactivating ID cards, adding further physical security to entrances/exits, alerting the Federal Protective Service, developing or implementing special instructions, reminders, and training, as appropriate.

VI. Notification of Individuals

Affected individuals will be notified if, after evaluating the risks to the affected individuals, the BRT determines that:

- (1) PII was, or is reasonably believed to have been, acquired by an unauthorized person and that the information could be used for fraudulent purposes; or
- (2) PII was, or is reasonably believed to have been, acquired by an unauthorized person and its use is likely to lead to harm.

The SAOP will provide notice to individuals without unreasonable delay. The time between notification and the risk evaluation should not exceed 48 hours except in extraordinary cases where notification would impede investigation and/or law enforcement. However, any delay should not exacerbate risk or harm to any affected individual.

A. Notification Elements

The BRT will consider the following elements in the notification process. These elements will be analyzed in accordance with guidance set forth in OMB memorandum M-07-16:

- Timing of the notice;
- Source of the notice;
- Contents of the notice;
- Method of notification; and
- Preparation for follow-on inquiries.

In particular, the contents of any notice given by the agency to individuals will include the following:

B. Content of the Notice

- A brief description of what happened, including the date of breach and its discovery;
- To the extent possible, a description of the types of information that were involved in the breach;
- A brief description of what the agency is doing to investigate the breach, mitigate losses, and protect against further breaches;
- Point-of-contact information for individuals who have questions or need more information, including a toll-free number, Web site, and/or postal address;
- If the breach involved sensitive PII (i.e., SSN, medical or financial information) steps for individuals to undertake in order to protect themselves from the risk of ID theft, including how to take advantage of credit monitoring or other service(s) that the agency intends to offer, if any, and URL information for the EPA's Web site, including specific relevant publications; and
- A statement whether the information was encrypted or protected by other means, when such information would be beneficial and would not compromise the security of the system.

VII. Notification to Third Parties

The Agency is publishing a Federal Register notice to add a new general routine use that will allow it to disclose information in its systems covered under the Privacy Act to persons and entities that may be needed by the Agency to respond, prevent, minimize or remedy harm, resulting from an Agency breach or compromise of personally identifiable information. Notice to individuals and notice to third parties, including the timing, order, and content of such notice, will be carefully coordinated so that any ongoing investigations are not compromised, the risk of harm to individuals is minimized, and the information provided is consistent and accurate. Accordingly, the BRT will consider a wide variety of possible harms in determining whether external notification of a breach is necessary.

Notice to the following third parties may be required, depending on the nature of the breach:

<u>THIRD PARTY NOTIFICATION</u>	<u>ROLES AND RESPONSIBILITIES</u>
Law Enforcement	Depending on the nature of the breach, and, if possible criminal violations are apparent, the BRT will notify the OIG, which may choose to notify the EPA Security Officer, federal, state, or local law enforcement, including local police departments, Federal Protective Service (FPS), and the Federal Bureau of Investigation.
United States Computer Emergency Readiness Team (US-CERT)	Responsible for complying with all policies concerning the notification of incidents to US-CERT. Incidents involving PII will be reported to US-CERT as soon as practical. The Agency will not distinguish between potential and confirmed incidents for purposes of notifying US-CERT and will provide updates as necessary and appropriate in each case.
Media and the Public	Notice to the media and the public is the responsibility of the Director, Office of Public Affairs, in coordination with the BRT, including directing all meetings and discussions with the news media and public. This includes the issuance of press releases and related materials on www.epa.gov .
Financial Institutions	If the breach involves government-authorized credit cards, EPA must notify the issuing bank Agency's promptly as set forth in OMB memorandum M-07-16. The Office of the Chief Financial Officer will handle notifications and suspension of accounts. If the breach involves individuals' bank account numbers that are used in employment-related transactions (e.g., payroll), EPA will

ROLES AND RESPONSIBILITIES

notify the bank or other entity that handles that particular transaction for the Agency.

Appropriate Members of Congress

The Director, Office of Congressional Relations, in consultation with the BRT, is responsible for coordinating all communications and meetings with members of Congress and their staff. The BRT will notify the Director, Office of Congressional Relations immediately when an issue arises that may require communications with members of Congress and their staff.

Attorney General

The IG may notify the Office of the Attorney General of any criminal violations relating to the disclosure or improper use of Privacy Act information or PII, as required by the Inspector General Act of 1978, 5 U.S.C. Appendix Section 3, as amended.

In addition, the BRT will work closely with other Federal agencies, offices, and teams as appropriate.

VIII. Documentation of Breach Notification Response

Activities documenting the Agency's investigation and response to breaches are Agency records. The BRT Chair, OIG, and other appropriate officials and staff, will ensure that accurate records are maintained of their activities to document the Agency's response to all breaches reported under this procedure.

In accordance with the Privacy Act of 1974 and the Federal Records Act, such records will be generated, compiled and maintained in a manner sufficient to safeguard the financial, legal or other rights of individuals, if any, affected by the breach, including any parallel law enforcement investigations, litigation, or other pending action. At the same time, such documentation will be maintained no longer than required by applicable records retention schedules to ensure that any sensitive PII in such records is not unnecessarily retained or exposed to a risk of breach. Records will be destroyed only in accordance with approved and secured methods designed to ensure against inadvertent disclosure, theft, or other compromise of personal or other nonpublic information. Files will be maintained and disposed of in accordance with the applicable EPA records control schedule(s).

IX. Evaluation of Breach Response

The development and implementation of this procedure is an ongoing process and not a one-time exercise. Accordingly, following the handling and disposition of all suspected or actual breaches reported under this procedure, the BRT, BET, EPA Call Center, and CSIRC Team will evaluate their responses considering tasks that could have been conducted more effectively and efficiently and make improvements or modifications to this procedure as appropriate. Each office participating in handling the breach will also review its procedures to make the same evaluations.

X. Roles and Responsibilities

A. Breach Response Team (BRT)

The Senior Agency Official Privacy will Chair the BRT, preside over meetings, and initiate responses to incidents as appropriate. The Chief Privacy Officer in OEI will serve as the chair of the BRT in the absence of the SAOP. A list of current BRT members by name and title is attached to the procedure and are available at <http://epa.intranet/privacy/members>.

The BRT will conduct any additional analysis and recommend a course of action on behalf of the Agency in response to the breach. In the event of a confirmed breach of SSNs or other Agency sensitive PII, the BRT will promptly convene the team, conduct a risk analysis and timely implement a risk-based response, tailored to the specific breach.

Consistent with OMB memorandum OMB M-07-16 and Agency roles and responsibilities, the EPA BRT permanent core members will consist of the following individuals (or their designees):

Senior Agency Official Privacy (SAOP)

Inspector General (IG)

General Counsel (GC)

Director, Office of Public Affairs (OPA)

Chief Privacy Officer (OIC)

Chief Information Security Officer (CISO)

Deputy Associate Administrator, Office of Congressional Affairs

Deputy Assistant Administrator, Office of Administration & Resources Management

Chief Financial Officer (CFO)

Senior Official from Program Office where the breach occurred

B. Breach Evaluation Team

The Breach Evaluation Team (BET) will be co-chaired by the Director, Technology and Information Security Staff (OTOP) and the Chief, Records, FOIA and Privacy Branch (OIC) and staffed by privacy and security staff, along with others who may be needed to respond to the subject incident. The TISS Director will convene the BET when the CSIRC Team reports suspected or confirmed PII breaches. The BET will review the investigatory findings of the CSIRC Team, conduct the risk analysis of the suspected or confirmed breach and report its findings to the Agency SAOP. BET core members:

Chief, Technology and Information Security Staff (TISS) & Staff
Chief, Records, FOIA and Privacy Branch (RFPB) & Privacy Staff
ISO of subject organization
Liaison Privacy Official of subject organization

C. Computer Security Incident Response Capability Team - The Computer Security Incident Response Capability Team (CSIRC) provides contract support to OEI's Office of Technology Operations and Planning. CSIRC is the Agency's official liaison with the Department of Homeland Security's US-CERT. The CSIRC Team will investigate all reported breaches of PII and provide its findings to OEI.

D. EPA Call Center – The Call Center will prioritize reported incidents and forward PII breach reports to the CSIRC Team for further evaluation and investigation, as appropriate.

E. Office of the Inspector General - The OIG will play a central role in the investigation of any breach. When appropriate, the OIG/OI will assist the BRT in making a determination of the risk of harm and the need for providing individuals with notice. In addition, in accordance with the Inspector General Act and other applicable laws, the IG will conduct an evaluation to determine, among other things: (1) if the theft of PII was intentional; (2) if employee misconduct was involved; (3) if the theft or compromise was a one-time incident or part of a broad based criminal effort; (4) if the incident is part of an ongoing investigation by the FBI, Secret Service, FPS or other federal, state, or local law enforcement; or (5) if notice to individuals or third parties would compromise an ongoing law enforcement investigation.

F. Office of General Counsel - The OGC will be responsible generally for providing legal support and guidance in responding to a suspected or actual breach.

G. Office of Public Affairs - The OPA will decide when and how the public would be notified in cases of a breach of PII.

H. Office of Environmental Information - The SAOP will chair the BRT and convene meetings of the BRT, as appropriate. The SAOP will take all necessary steps to contain, control and mitigate the risks from the breach and prevent further unauthorized access to or use of individual's information. As chair of the BRT, the SAOP ensures that appropriate and adequate records are maintained to document

the initial analysis of the suspected breach and the BRT's response to all confirmed breaches reported under this procedure. The SAOP ensures appropriate and prompt notification in the event of a breach of PII commensurate with the risk of harm to the individual and consistent with Federal and Agency standards and requirements. The SAOP will be responsible for making the final decisions on the notification of individuals.

- OTOP will have the Agency lead for determining whether the breached data system was properly secured and whether the information was properly encrypted or otherwise rendered unusable. OTOP will ensure that, when practicable, appropriate enterprise technology safeguards are identified and implemented to protect sensitive electronic information from inappropriate disclosure, misuse, or other security breaches, in accordance with Federal and Agency security standards and requirements.
- OEI's **Office of Information Collection** will chair the BRT when the SAOP is absent. OIC will support OTOP, as appropriate, with risk mitigation and have the Agency lead for ensuring that adequate safeguards are in place to prevent further breaches of paper PII records.

I. Office of Administration and Resources Management – OARM will respond to breaches involving the physical security of EPA buildings and provide information needed by the BRT to contact employees who are affected by the incident.

J. Office of Regional Counsel – The Office of Regional Counsel will provide legal support and guidance in responding to a suspected or actual breach which occurs in an EPA regional office and participate in BET meeting.

K. Office in Which Breach Occurred - The Office in which the breach occurs will report the breach to the appropriate ISO and the EPA Call Center and participate in follow up activities as needed; participate in the BET meetings; conduct follow-up activities, implement remedial action, ensure appropriate safeguards are in place; conduct lessons learned, as appropriate, and draft the response letter to affected individuals, if required.

L. Other EPA Organizations - The BRT may involve other EPA organizations in the breach response, as necessary.

XI. Rules and Consequences

Employees, managers and supervisors will be informed and trained by the Agency's Privacy and Security staffs regarding their responsibilities to safeguard PII and report suspected or known incidents.

Individuals must understand they are subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring.

Consequences will be commensurate with level of responsibility and type of PII involved. The particular facts and circumstances including whether the breach was intentional will be considered in taking appropriate disciplinary actions.

XII. Definitions

- 1. Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual.
- 2. Sensitive Personally Identifiable Information** - Sensitive PII is a subset of Agency-held PII which requires additional levels of security in accordance with the requirements set forth in section 6 of the Agency's Privacy Policy. EPA classifies sensitive PII as Social Security numbers, or comparable identification numbers, financial information associated with individuals and medical information associated with individuals.
- 3. Breach and/or Incident** – The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII or Privacy Act information, whether physical or electronic.