EPA INFORMATION PROCEDURES

EPA Classification No.: CIO 2151-P-02.2	CIO Approval Date: 08/7/2013
CIO Transmittal No.: 13-006	Review Date: 08/7/2016

Procedure for Responding to Breaches of Personally Identifiable Information (PII)
Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated

1. PURPOSE

This procedure identifies the steps the Environmental Protection Agency (EPA) will take to respond to suspected or confirmed breaches of personally identifiable information (PII). This procedure sets out the roles and responsibilities for reporting and responding to PII breaches so that Agency officials, employees and other individuals will be able to quickly and effectively respond to any breach for which the EPA is responsible.

2. SCOPE AND APPLICABILITY

This procedure applies to Agency employees, grantees and contractors and supplements other Agency procedures identified in Section 7 below for protecting PII and responding to incidents regarding the security of such information.

3. AUDIENCE

All Agency officials, staff, contractors and others working on behalf of the Agency.

4. BACKGROUND

On February 11, 2005, the Office of Management and Budget (OMB) required federal agencies to designate a senior official with overall agency-wide responsibility for privacy issues. EPA's Assistant Administrator of the Office of Environmental Information (OEI) and Chief Information Officer (CIO) was designated as EPA's Senior Agency Official for Privacy (SAOP). The SAOP is responsible for ensuring the implementation of information privacy protections, including full compliance with federal laws, regulations, and policies relating to information privacy.

On May 22, 2007, OMB issued memorandum, M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" requiring agencies to develop and implement procedures for responding to PII breaches, including establishing a core management group to respond to the loss of PII should a breach occur. OMB recommended that the core management group include, at a minimum, the agency's chief information officer, chief legal officer, inspector general, and other senior management officials (or their designees) with expertise in information technology, legal authorities, and law enforcement necessary to respond to a breach. EPA established a core group of Agency senior leaders to respond to breaches of PII, called the Breach Notification Team (BNT). Members of the BNT are defined later in this procedure.

The Agency must be prepared to act promptly when breaches occur in order to mitigate

potential risks to affected individuals. To expedite review for PII incidents, the Agency established the Breach Evaluation Team (BET) and the Breach Evaluation Team Executive Committee (BET EX). The BET reviews suspected, possible or confirmed breaches of all PII and decides the Agency's response to breaches of non-sensitive PII. The BET provides the BET EX recommendations for Agency responses to breaches of sensitive PII. The BET EX acts on behalf of the BNT to respond to suspected, possible or confirmed sensitive PII breaches. Only in circumstances defined later in this procedure will the BNT need to convene. For the definition of sensitive and non-sensitive PII, as well as other terms used in this procedure, see section 9 below. For the definition of roles and responsibilities, see section 8 below. This procedure:

1. Establishes and defines the membership of the Agency's core management group for PII breaches (BNT);
2. Establishes a senior-level management team to act on behalf of the BNT when the breach involves *sensitive* PII (BET EX);
3. Establishes and defines the management team to review and evaluate all known and suspected breaches reported to the EPA Call Center and act on behalf of the BET EX when the breach involves *non-sensitive* PII (BET);
4. Establishes the process for reporting known or suspected PII incidents;
5. Establishes the process the Agency will use to evaluate the likelihood of risk of harm to individuals affected by a breach;
6. Establishes time frames for the Agency to decide how the breach will be addressed;
7. Establishes a process for organizations to appeal decisions issued by the BET and BET EX;
8. Establishes the process and timeframes for notifying affected individuals;
9. Establishes the requirement for offering credit-monitoring services; and
10. Identifies roles and responsibilities of response teams, key Agency offices, and third parties that may be involved in breach response, mitigation and notification activities.

5. AUTHORITIES

A. OMB Memorandum, M-11-02, FY 2010 Sharing Data While Protecting Privacy (November 3, 2008).

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

C. OMB Memorandum, "Recommendations for Identity Theft Related Data Breach Notifications," September 20, 2006 PDF).

D. OMB Memorandum, M-06-19, "Reporting Incidents Involving PII and Incorporation of Costs for Security in Agency Information Technology Investments," July 12, 2006.

E. OMB Memorandum M-06-16, "Protection of Sensitive Agency Information," June 23, 2006.

F. OMB Memorandum M-06-15, "Safeguarding Personally Identifiable Information," May

22, 2006.

G. OMB Memorandum M-05-08, "Designation of Senior Agency Officials for Privacy," February 11, 2005.

H. OMB Memorandum M-01-05, "Guidance on Inter-Agency Sharing of Personal Data Protecting Personal Privacy," December 20, 2000.

I. OMB Circular No. A-130 Appendix I to OMB Circular No. A-130 "Federal Agency Responsibilities for Maintaining Records About Individuals".

6. PROCEDURES

I. Reporting Breaches

Pursuant to EPA's Privacy Policy, all Agency officials, staff, contractors and others working on behalf of the Agency are directed to immediately report any suspected or known breach of PII. Incidents must be reported to the EPA Call Center (1-866-41-4372, Option 1) as soon as a breach is suspected or known.

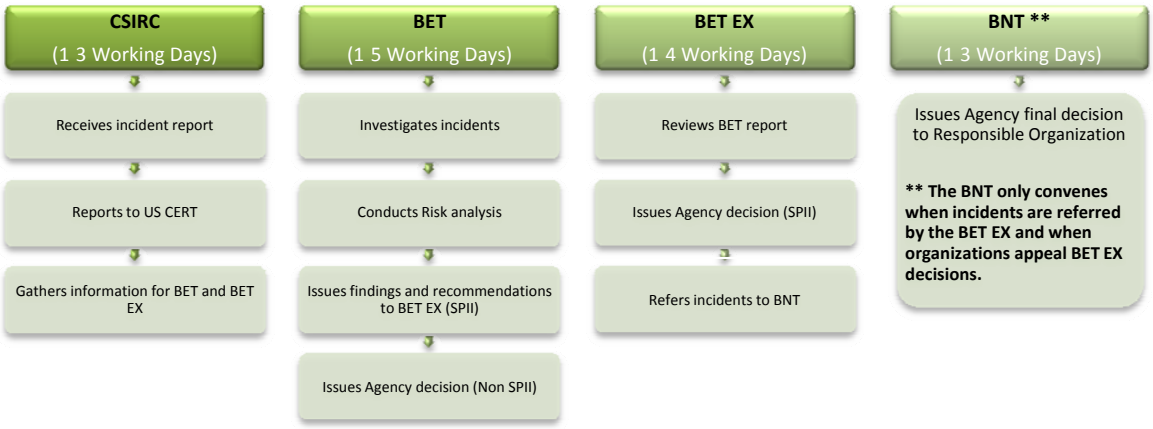
The EPA Call Center

When the EPA Call Center receives a report of a possible PII breach, it will obtain the information necessary from the caller to identify the type of PII involved and nature of the reported incident. The Call Center will obtain the following information in order to assist in determining whether a breach has occurred:

- Type of PII (e.g., social security number, home address, home e-mail address);
- Date and time of incident;
- Nature of incident and the means by which the incident occurred;
- How the information was breached;
- Whether there was a system or network intrusion;
- Whether the incident involved paper documents;
- Person responsible for the incident (if known or can be identified);
- Person who reported incident, including contact information;
- Person who discovered incident, including contact information;
- Number of individuals whose PII may be affected;
- Number of records potentially affected;
- Accessibility of the PII information (e.g., paper records, unencrypted or encrypted files, etc.);
- Whether the information was encrypted;
- Whether the device was password protected;
- Other relevant information.

The Call Center staff will immediately transfer the incident report to the Agency's Computer Security Incident Response Capability (CSIRC) Team.

II. Responding to Reported Breaches



Each of the above response teams will complete their actions as quickly as possible and no later than the maximum number of working days specified.

When a breach that presents an ongoing or imminent risk of harm is reported to CSIRC, the Agency will take immediate steps to contain, control and address the cause of the breach. In these cases, the breach response teams will determine any additional actions required and whether notification and/or credit monitoring will be provided.

A. Computer Security Incident Response Capability (CSIRC) Team

CSIRC will work with the Breach Evaluation Team (BET) and others, when so directed, to investigate breach incidents involving sensitive PII. If the incident involves a possible criminal violation, CSIRC will immediately notify the Office of the Inspector General, Office of Investigations (OIG/OI) and the Office of General Counsel (OGC). CSIRC may be contacted to gather additional information by the BET or the BET EX, as needed. (See II.C. and D. for BET and BET EX discussion.)

1) Sensitive PII. When sensitive PII is involved, CSIRC will report the incident to the United States Computer Emergency Readiness Team (US-CERT) within one hour of discovery and immediately forward the incident report to the BET. CSIRC may be requested to obtain additional information needed by the BET to complete its findings or the BET EX during its decision-making.

2) Non-sensitive PII. CSIRC will forward reports involving non-sensitive PII directly to the BET for investigation.

B. Breach Evaluation Team (BET)

The BET is chaired by the Freedom of Information Act (FOIA) and Privacy Branch Chief in the Office of Information Collection, Office of Environmental Information and co-chaired by

the Deputy Senior Agency Information Security Officer. The Primary Information Security Officer of the responsible organization(s), the Agency Privacy Officer, Liaison Privacy Official(s) and others, for example, the Office of Technology Operations and Planning, may be needed as subject matter experts to respond to the subject breach and will serve a consultative role.

When a PII breach is confirmed, the BET will immediately notify the Liaison Privacy Official (LPO), Information Security Official (ISO) and the Information Management Official (IMO) from the responsible organization. The Senior Information Official (SIO) also will be notified if immediate action is required to address the incident and/or if the breach is believed to be high risk.

If the breach involves sensitive PII, The BET will review the incident report submitted by CSIRC and ensure there is sufficient information provided to evaluate the likelihood of risk of harm to the affected individual(s) and the Agency. The BET will conduct a risk analysis and issue a report of its findings and recommendations to the Breach Evaluation Team Executive Committee (BET EX), including whether the risk can be mitigated, whether the individual(s) should be notified and whether credit monitoring or other remedies to the affected individual(s) should be offered. The BET will issue its findings and recommendations report to the BET EX no later than five working days after receiving the incident report from CSIRC.

If the breach involves non-sensitive PII, the BET will review the incident report submitted by CSIRC and ensure there is sufficient information provided to evaluate the likelihood of risk of harm to the impacted individual(s) and the Agency. The BET will conduct a risk analysis to determine the course of action to be taken by the Agency and issue a decision memorandum to the office director of the responsible organization. The BET will issue its decision to the responsible organization no later than five working days after receiving the incident report from CSIRC. However, when the BET determines that notification to affected individuals may be warranted, it will forward its findings and recommendations report to the BET EX. (Only the BET EX and the BNT have authority to decide whether to notify affected individuals.)

C. Breach Evaluation Team Executive Committee (BET EX)

The BET EX decides how the Agency will respond to breaches of sensitive PII, including whether notification to affected individuals and/or credit monitoring are warranted.

The BET EX is chaired by the Chief Privacy Officer (CPO) who is also the Director, Office of Information Collection, and comprised of the Associate General Counsel, General Law Office, the Senior Agency Information Security Officer, a senior official from the current OEI Lead Region, and a senior official from the responsible organization. Additional subject matter experts may be called upon from the Technology and Information Security Staff to consult or provide advice.

The BET EX will review the BET's report and background documents to determine the necessary course of action. The members will consider the context in which the breach

occurred; the number of individuals involved; and all mitigating factors to determine the risk of harm to the affected individual(s) and to the Agency. In addition to the harm of identity theft and financial harm, other harms will be considered, such as harm to reputation and the potential for harassment or prejudice, particularly when medical or financial information is involved. Unlike the BET, which uses a risk-based approach to evaluate the likelihood of harm, the BET EX may consider not only the risk analysis findings of the BET, but will consider **all** potential harms including risk of reputation to the Agency.

The BET EX shall attempt to reach a consensus on the Agency's response. If a consensus cannot be reached, the Chair must call for a vote requiring a simple majority. To avoid a potential conflict of interest, the responsible organization's member of the BET EX does not participate in reaching consensus and cannot vote. The decision memorandum is prepared by the BET EX Chair and issued to the Office Director of the responsible organization. The memorandum will transmit the Agency's findings and decision, along with instructions, as appropriate. The BET EX and the BET are copied on the decision memorandum. The BET EX will issue its decision to the responsible organization in writing no later than four working days after receiving the BET report.

D. The Breach Notification Team (BNT)

The BNT is chaired by the Agency Chief Information Officer (CIO) who is also the Senior Agency Official for Privacy (SAOP). The Agency SAOP convenes and chairs the BNT; the Principle Deputy Assistant Administrator for OEI chairs in the absence of the SAOP. The BNT is the Agency's core management group (defined by OMB in Memorandum M-07-16). The SAOP makes final decisions after receiving input from BNT members. The BNT is convened only when 1) an incident is referred by the BET EX for a decision or 2) the responsible organization appeals the decision of the BET EX to the SAOP. The BNT will issue its decision to the responsible organization in writing no later than three working days after receiving the BET EX report. The BNT is comprised of a senior Agency official from each office below:

Office of Environmental Information (OEI)
Office of Inspector General (OIG)
Office of General Counsel (OGC)
Office of External Affairs and Environmental Education (OEAEE)
Office of Congressional and Intergovernmental Relations (OCIR)
Office of Administration and Resources Management (OARM)
Office of the Chief Financial Officer (OCFO)
Senior Official from Responsible Organization
Senior Official from Lead Region for the Office of Environmental Information

E. Responsible Organization

The responsible organization (as defined in Section 8, below) will take all necessary steps to contain, control and mitigate the risks from the breach and prevent further unauthorized access to or use of PII. The office will manage notification activities; conduct any necessary and appropriate follow-up; implement remedial actions; ensure that appropriate safeguards are in place; and provide credit monitoring, when required.

The responsible organization will be invited to participate in BET, BET EX and BNT meetings to answer questions, provide additional information and help inform decisions. The responsible organization must implement all decisions received from the BET, BET EX or BNT as directed. If the responsible organization disagrees with the findings and recommendations, it must appeal the decision within three working days. See Section F. below.

The responsible organization will provide and pay for notification expenditures, including credit monitoring services, within three working days after receiving the Agency's decision, except in extraordinary cases such as where a new contract vehicle is required to provide the credit monitoring services, contact information for the individuals cannot be easily obtained or the immediate notification would impede an investigation or law enforcement effort. The Office of General Counsel, Agency public relations and labor and employee relations staff will, when necessary and/or appropriate, review notification messages before they are released. The responsible organization will also provide a record of final disposition and/or notification to the Agency's Privacy Officer.

F. Appealing Agency Decisions

The responsible organization may appeal decisions issued by the BET or BET EX. All appeals must be in writing and provide the rationale for the appeal.

Appealing a BET Decision

.

If the responsible organization does not agree with a decision issued by the BET, it may appeal the decision to the BET EX within three working days after receipt. The appeal must be in writing and provide an explanation for the disagreement. The BET EX has three working days to issue a decision to the responsible organization. The decision issued by the BET EX is the Agency's final decision when BET decisions are appealed.

Appealing a BET EX Decision

If the responsible organization does not agree with a decision issued by the BET EX, it may appeal the decision to the SAOP within three working days after receipt. The appeal must be in writing and provide an explanation for the disagreement. The SAOP will convene the BNT within two working days after the appeal is received. The BNT has three working days to issue a decision to the responsible organization. The decision issued by the BNT is the Agency's final decision.

BNT Decisions

All decisions issued by the BNT are final and cannot be appealed.

The SAOP is authorized and required to notify the Deputy Administrator when responsible organizations are non-compliant or do not respond to Agency decisions for more than five working days.

III. Taking Steps to Contain and Control the Breach

A. Incidents Involving Electronic and Paper Breaches

The responsible organization will coordinate response activities with appropriate Agency organizations to ensure that appropriate steps are taken to contain and control the breach and to determine safeguards required to avoid such a breach from reoccurring. Steps may include: (1) monitoring, and possibly freezing, or closing, affected accounts; (2) modifying computer access controls or physical access controls; and (3) taking other necessary and appropriate actions. These steps will be taken without undue delay and consistent with current requirements under the National Institute of Standards and Technology (NIST), the Federal Information Processing Standards (FIPS), OMB Directives and Agency policies.

B. Incidents Involving Physical Security Breaches

If the incident involves a physical security breach that affects PII, the EPA Physical Security Staff will ensure that necessary steps are taken to contain and control the breach and prevent further unauthorized access. At EPA headquarters, this responsibility falls under the Office of Administration and Resources Management (OARM); the responsibility may be located in other organizations in EPA regional offices. Steps may include changing locks or key codes, securing/locking file cabinets, deactivating ID cards, adding further physical security to entrances/exits, alerting the Federal Protective Service, and developing special instructions, as appropriate.

C. Incidents Involving Electronic Official Personal Files (eOPFs)

OARM is delegated the authority, by the SAOP, to directly respond to incidents involving the misfiling of PII in electronic official personnel files (e-OPFs). OARM will notify employees when their PII is misfiled without BET EX review. At the end of each fiscal year, OARM must provide the Agency Privacy Officer the number of eOPF breaches they addressed during the fiscal year. If the incident is not a misfiling of an e-OPF, the breach will be reported and managed under this procedure.

IV. Assessing Risk of Harm

To determine whether the Agency will notify affected individuals, the Agency must first assess the risk of harm to the individual(s) affected by the breach**.** The BET uses a risk management approach based on guidelines published by the National Institute of Standards and Technology (NIST-800-12) to assess the likelihood of harm to individuals or organizations following breaches of PII. The BET uses the impact levels of low, moderate and high to rate the potential harm that could result if the PII were inappropriately accessed, used or disclosed. The assessment is used by the BET to determine vulnerability, threat and likelihood of harm by considering the following:

- Nature of the data elements breached (e.g., sensitive PII, non-sensitive PII, aggregate PII elements)
- Likelihood the information is readily accessible and usable (e.g., encrypted, unencrypted, paper, password protected)

- Ability of the Agency to mitigate the risk of harm (e.g., Internet vs. Intranet exposure)
- Number of individuals affected (influences risk response and method of notification)

The BET considers a range of recommendations depending on the level or risk:

- Low risk – Privacy training for EPA staff and others, discussions, counseling, instructions
- Moderate risk – Notification to affected individual(s), privacy training, discussions, counseling instructions
- High risk – Credit monitoring, notification to affected individual(s), privacy training

The BET EX and/or BNT may review the BET's risk assessment to inform decisions regarding notification and other response actions. In addition to the harm of identity theft, the Agency may also consider other possible harms to individuals such as harm to reputation and the potential for harassment or prejudice (such as in hiring practices). After assessing relevant risk factors, the BNT and/or BET EX will decide whether to notify affected individuals and/or take additional actions.

V. Notifying Individuals

Notification allows the affected individual(s) to take steps to help protect themselves from the potential consequences of the breach and to mitigate potential harm resulting from the breach. In addition to notifying individuals, the Agency may consider other options to minimize potential harm including providing credit monitoring services if it is determined that such services are required to mitigate potential damage due to the breach. See *Agency Instructions for Credit Monitoring* at http://intranet.epa.gov/privacy/guidance_document.htm.

Notification letters must be signed by an Office Director or higher with a copy to the Agency Privacy Officer. Depending on the circumstances and/or size of the breach, the BET EX, at its discretion, may request the appropriate Assistant Administrator, Deputy Assistant Administrator or the SAOP (CIO) to sign the notifications to the individuals affected by the breach.

A. Content of the Notice

The contents of any written notice given by the Agency to individuals will include the following:

- 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, website, and postal address;
- A statement concerning whether the information was encrypted or protected by other
means when sharing such information would be beneficial and would not compromise the security of the system; and
- If the breach involved sensitive PII (i.e., social security number, medical or financial information associated with an individual) suggested steps for individuals to take in order to protect themselves from the risk of identity theft, including how to obtain credit monitoring services offered by the Agency. (See Section VI. B. below.) See sample notice at http://intranet.epa.gov/privacy/guidance_document.htm (templates and examples.)

B. Means of Providing Notification

- **First-Class Mail.** First-class mail notification to the last known mailing address of the individual(s) in the Agency's records is the primary and preferred means to provide notification. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient.

- **E-Mail.** The Agency may use e-mail to notify Agency employees, in addition to regular first-class mail. Notification by e-mail must be documented with a "return receipt" to determine when/if the message is received by the intended recipient. If a non-employee provides an e-mail address and has expressly given consent to use e-mail as the primary means of communication with the Agency, and no known mailing address is available, notification by e-mail alone may be appropriate.

- **Telephone.** Telephone notification may be appropriate in cases where urgency dictates immediate and personalized notification and/or when a small number of individuals are affected. The content of all telephone notifications will be confirme**d** in writing to the affected individuals. Regular first class or e-mail notification will follow any telephone notice.

VI. Mitigating the Risk of Harm

A. Credit Monitoring

When the Agency determines that credit monitoring is warranted, **i**t will be provided to any affected individuals for at least one year free of charge. Affected individuals must notify the Agency, as defined in the notification letter, that credit monitoring is requested. (See http://intranet.epa.gov/privacy/Attachments/GSA_Credit_Monitoring_BPA_&_Agency_Instructions.pdf)

B. Affected Individuals

If not covered by the credit monitoring service, or if credit monitoring is not provided by the Agency, individuals affected by the breach may wish to take the following steps. EPA will notify them of these options:

- Contact financial institutions
- Monitor financial account activity
- Request a free credit report
- Place an initial fraud alert on credit reports
- Place a freeze on their credit file, for residents of states in which it is authorized under state law
- Review additional resources at www.idtheft.gov

C. Other Notifications

The Agency must establish agreements (e.g., Memoranda of Understanding, Interconnection Security Agreements) with external groups when PII is involved; such an agreement is intended to
identify the roles and responsibilities of all parties concerning handling a potential PII breach. These agreements must be reviewed by the Agency's Privacy Officer prior to approval.

The Agency may disclose information to appropriate agencies, entities, and persons when it is suspected or confirmed that: (1) the security or confidentiality of information in the system has been compromised; (2) there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of the system or other systems or programs that rely upon the compromised information; or (3) third parties are necessary to assist in connection with the Agency efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

When the Agency decides that notice to third parties is required, the timing, order, and content of such notice, will be carefully coordinated with appropriate organizations (e.g., OGC, OEI, OEAEE, OCIR, OIG, etc.) so that any ongoing investigations are not compromised; the risk of harm to individuals is minimized; and the information provided is consistent and accurate. The Agency will work closely with other federal agencies and offices, as appropriate. Third party notifications may include:

Members of Congress - The Director, Office of Congressional and Intergovernmental Relations (OCIR), in consultation with the responsible organization and either the BET EX or BNT, is responsible for coordinating all communications and meetings with members of Congress and their staff. The representative of the responsible organization will immediately notify the Director, (OCIR) when an issue arises that may require communications with members of Congress and their staffs.

Attorney General - The OIG may notify the Office of the Attorney General of any criminal violations relating to the disclosure or improper use of PII, as required by the Inspector General Act of 1978, as amended, 5 U.S.C. Appendix Section 4.

Financial Institutions – The Office of the Chief Financial Officer (OCFO) will handle notifications and suspension of accounts, if the breach involves government-authorized credit cards. If the breach involves individuals' bank account numbers, the individuals are responsible for taking the steps outlined in Section VI. B. of these procedures.

Law Enforcement – Law enforcement offices will be notified if possible criminal violations are apparent. Such offices include the Agency's Office of Inspector General (OIG); the EPA Security Office; federal, state, or local law enforcement, including local police departments; Federal Protective Service (FPS) and/or the Federal Bureau of Investigation.

Media and the Public - The Director, OEAEE, in coordination with the responsible organization and OEI, has the lead for communicating with the media and the public.

VII. Documenting Breach Response Activities (Recordkeeping)

In accordance with the Federal Records Act, activities documenting the Agency's investigation and response activities are Agency records. The responsible organization, BET, BET EX, BNT, EPA Call Center, CSIRC and others involved in breach response activities must maintain records of their actions according to Agency records retention policies.

The responsible organization must provide a copy of the final notification letter and a record of actions taken in response to the decisions issued by the BET, BET EX and BNT to the Agency's Privacy Officer. All files will be maintained and disposed of in accordance with the Federal Records Act and applicable EPA records control schedule(s).

VIII. Evaluating Breach Response

The handling and disposition of all suspected or actual breaches reported under these procedures will be periodically evaluated by the BET and the Privacy Officer to determine whether tasks can be conducted more effectively and to make modifications to the processes as appropriate.

7. RELATED DOCUMENTS

A. Agency Network Security Policy, Directive 2150 (PDF).

B. EPA Order 1900.1A CHG 2 Interacting With Contractors (PDF).

8. ROLES AND RESPONSIBILITIES

Agency Employees - Agency employees are responsible for immediately reporting suspected or known breaches of PII to the primary Information Security Officer (ISO) and the EPA Call Center at 1-866-411-4372, Option 1 as soon as the breach is discovered. A list of the ISOs for EPA organizations is available at http://intranet.epa.gov/itsecurity/compoversightassit/iso-list.html.

Agency Privacy Officer – The Agency Privacy Officer develops and implements response procedures to be followed in the event of a PII breach; provides subject matter expertise to Agency breach response teams; provides guidance and support to responsible organizations, as appropriate.

Breach Evaluation Team (BET) - The BET decides how the Agency will respond to incidents involving non-sensitive PII and makes recommendations to the Breach Evaluation Team Executive Committee when sensitive PII is involved**.** The BET is chaired by the Chief, FOIA and Privacy Branch in the Office of Information Collection (OIC) and co-chaired by the Deputy Senior Agency Information Security Officer. The responsible organization, Information Security Officers (ISOs), Liaison Privacy Officials (LPOs) and others needed to respond to the subject breach serve as ad hoc members, as needed.

Breach Evaluation Team Executive Committee (BET EX) - The BET EX decides how the Agency will respond to breaches of sensitive PII, when notification is warranted, and whether credit monitoring will be offered to the affected individuals. The BET EX is chaired by the Director, Office of Information Collection within the Office of Environmental Information (OEI) and comprised of a senior official from the Office of General Counsel, the Senior Agency Information Security Officer (SAISO), a senior official from the current OEI lead region and a senior official from the responsible organization.

Breach Notification Team (BNT) - The BNT advises the SAOP when incidents are referred by the BET EX for a decision and when an initial decision issued by the BET EX is appealed by the responsible organization. The BNT is chaired by the SAOP and is comprised of senior officials from Agency organizations, noted below. The SAOP will issue final Agency decisions when incidents are referred by the BET EX and when appeals are received on decisions made by the BET EX. The Deputy Assistant Administrator for OEI chairs the BNT in the absence of the SAOP. (See http://intranet.epa.gov/privacy/BNT.htm for current list of BNT members by name and title.)

Office of Environmental Information (OEI)
Office of Inspector General (OIG)
Office of General Counsel (OGC)
Office of External Affairs and Environmental Education (OEAEE)
Office of Congressional and Intergovernmental Relations (OCIR)
Office of Administration and Resources Management (OARM)
Office of the Chief Financial Officer (OCFO)
Senior Official from the Responsible Organization (unless one of the above organizations).

Computer Security Incident Response Capability Team (CSIRC) - CSIRC provides incident management support to the Agency and reports breaches of sensitive PII to the Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT). The CSIRC
team will investigate all reported breaches of sensitive PII and forward non-sensitive breach reports to
the Breach Evaluation Team (BET).

Contractors - Contractors are responsible for reporting any suspected or known breach of PII, as soon as the incident is discovered, to the EPA Call Center (1-866-411-4372, Option 1). Contractors must immediately inform their Contracting Officer (CO) or CO Technical Representative (COTR) after reporting the incident to the Call Center.

Chief Privacy Officer (CPO) – The CPO is the Office of Information Collection's Officer Director. The CPO chairs the BET EX Committee and leads the Agency's efforts to ensure that adequate safeguards are in place to prevent breaches of both electronic and paper PII records, including training and awareness.

Deputy Administrator - The Deputy Administrator will issue final Agency decisions when the SAOP presents referrals of willful inaction by the responsible organization.

Deputy Assistant Administrator (DAA), Office of Environmental Information - The DAA for OEI will chair the BNT when the SAOP is not available.

EPA Call Center – The EPA Call Center receives reports of incidents and forwards PII breach reports to the CSIRC Team and BET for further evaluation and investigation, as appropriate**.**

Information Management Officer (IMO) – IMOs are responsible for implementing information management functions, including privacy requirements, in their organizations. IMOs are the primary organizational points of contact for the Agency Privacy Officer.

Information Security Officer (ISO) - ISOs are responsible for information security in their organizations and will work with CSIRC and the BET to address PII incidents involving electronic systems under their purview.

Liaison Privacy Official (LPO) - LPOs administer the day-to-day privacy activities in their programs and regions, assist with breaches and are the primary points of contact for the National Liaison Privacy Official.

Office of Administration and Resources Management (OARM) - OARM is delegated the authority, by the SAOP, to respond to incidents involving the misfiling of PII in electronic official personnel files (e-OPFs) without BET EX review. OARM is responsible for the physical security of EPA buildings and providing contact information, when required, to locate employees who are affected by the breach. OARM is a core member of the BNT.

Office of General Counsel (OGC) - OGC is responsible for providing legal support and guidance in responding to a suspected or known breach, as well as for participating on the BET EX and the BNT. OGC is a core member of the BNT.

Office of Inspector General (OIG) - The OIG/Office of Investigations will assist CSIRC with its investigation, when needed. OIG may conduct an evaluation to determine, among other things, if: (1) a theft of PII was intentional; (2) employee misconduct was involved; (3) a theft or compromise was a one-time incident or part of a broad-based criminal effort; (4) an incident is part of an ongoing investigation by the FBI, Secret Service, FPS or other federal, state, or local law enforcement; or (5) notice to individuals or third parties would compromise an ongoing law enforcement investigation. OIG is a core member of the BNT.

Office of External Affairs and Environmental Education (OEAEE) - OEAEE will advise OEI concerning external notifications, including the strategy for notifying the media and posting information to OEI's homepage, as appropriate. OEAEE is a core member of the BNT.

Office of Regional Counsel (ORC) - ORC will provide legal support and guidance in responding to a suspected breach, when it occurs in an EPA regional office, and will participate in BET, BET EX, and/or BNT meetings, as required.

Office of Technology and Operations Planning (OTOP) - OTOP, in coordination with the SAISO, will ensure that appropriate enterprise technology safeguards are identified and implemented to protect electronic information from inappropriate disclosure, misuse, or other security breaches, in accordance with Federal and Agency security standards and requirements.

Responsible Organization – The organization responsible for a breach is the owner of the information that was breached or of the system that was breached. [(See the Federal Information Security Management Act of 2002 (FISMA) and NIST 800-100 (National Institute of Standards and Technology)]. Typically, at EPA, they are the same organization; when they are not, the Information Owner has statutory accountability and responsibility. The responsible organization must implement and provide the resources to support the Agency's decision regarding breach response activities.

The Information System Owner is the agency official and organization responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. The information system owner has the following responsibilities related to system security plans:

- Develops the system security plan in coordination with information owners, the system administrator, the information system security officer, the senior agency information security officer, and functional "end users,"
- Maintains the system security plan and ensures that the system is deployed and operated according to the agreed-upon security requirements,
- Ensures that system users and support personnel receive the requisite security training (e.g., instruction in rules of behavior),
- Updates the system security plan whenever a significant change occurs, and
- Assists in the identification, implementation, and assessment of the common security controls.

The Information Owner is the Agency official and organization with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. The information owner has the

following responsibilities related to system security plans:

- Establishes the rules for appropriate use and protection of the subject data/information (rules of behavior),
- Provides input to information system owners regarding the security requirements and security controls for the information system(s) where the information resides,
- Decides who has access to the information system and what types of privileges or access rights.

Senior Agency Official for Privacy (SAOP) - The Agency CIO is the SAOP. The SAOP will chair the BNT and convene meetings of the BNT, as appropriate. 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 ensures that appropriate and adequate 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. The SAOP makes final decisions on Agency breaches with input from the BNT.

Senior Information Official (SIO) – SIOs are responsible for implementing Agency privacy regulations, policies and procedures within their respective organizations and for protecting individuals'
privacy by safeguarding personally identifiable information (PII).

U.S. Computer Emergency Readiness Team (US-CERT) - The Department of Homeland Security's United States Computer Emergency Readiness Team (US-CERT) leads efforts to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the Nation while protecting the constitutional rights of Americans. US-CERT strives to be a trusted global leader in cybersecurity - collaborative, agile, and responsive in a dynamic and complex environment.

9. DEFINITIONS

Aggregate PII. A collection of multiple personally identifiable information (PII) elements (e.g., name, address, date of birth, telephone number, etc.).

Breach. 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 whether paper or electronic.

Harm. Any adverse effect that would be experienced by an individual whose PII was the subject of a breach, as well as any adverse effects experienced by the organization that maintains the PII. Harm to an individual includes any negative or unwanted effects; examples of types of harm to individuals include, but are not limited to, the potential for blackmail, identity theft, physical harm, discrimination, or emotional distress.

Incident. An occurrence that actually or potentially, jeopardizes the confidentiality, integrity, or availability of an information system, or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Non-Sensitive Personally Identifiable Information (PII). Any information about an individual that is maintained by an agency that is used to distinguish, trace, or identify that individual, but which falls outside the scope of sensitive PII.

Personally Identifiable Information (PII). Any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify the individual, including personal information which is linked or linkable to that individual.

Record. Any item, collection or grouping of information about an individual maintained by an agency, e.g., the individual's education, financial transactions and medical, criminal or employment history; and that contains the individual's name, or any identifying number, symbol or particular assigned to the individual.

Risk-based approach. An activity, mechanism, or methodology that is designed to provide adequate security (as defined in OMB Cir. A-130, Appendix III) for the affected information technology and/or information resources. EPA uses the "PII Risk Assessment Tool" as its methodology for assessing potential risk of harm.

Sensitive Personally Identifiable Information (PII). Social Security numbers; financial information associated with individuals; and medical information associated with individuals. Sensitive PII is a subset of PII and requires additional levels of security controls.

10. WAIVERS

None.

11. RELATED POLICIES, STANDARDS AND GUIDANCE

- Privacy Policy (www.epa.gov/privacy/policy/index.htm)
- Privacy Threshold Analysis (http://intranet.epa.gov/privacy/guidance_document.htm)
- Privacy Impact Assessments (http://intranet.epa.gov/privacy/guidance_document.htm)

12. MATERIAL SUPERSEDED

CIO P- 2151-P-06

CIO P-2151-P-02.1

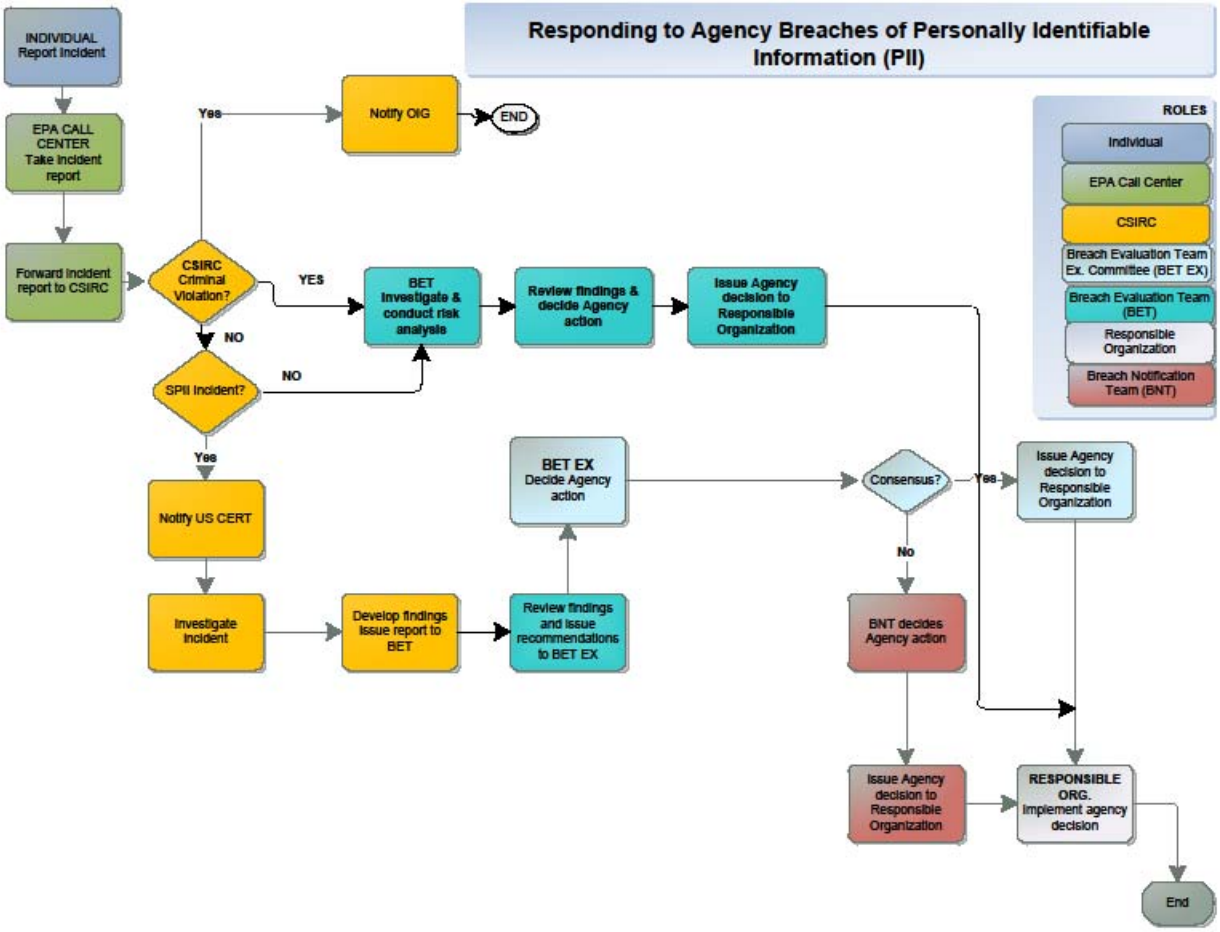
13. ADDITIONAL INFORMATION

See Appendix I for a flow diagram of the breach process.

EPA Classification No.: CIO 2151-P-02.2	CIO Approval Date: 08/7/2013
CIO Transmittal No.: 13-006	Review Date: 08/7/2016

Renee P. Wynn, Acting Assistant Administrator
and Chief Information Officer
Office of Environmental Information

Appendix I


Responding to Agency Breaches of Personally Identifiable Information (PII)
INDIVIDUAL Report Incident
EPA CALL CENTER Take incident report
Forward incident report to CSIRC
CSIRC Criminal Violation?
Yes
Notify OIG
END
YES
NO
BET Investigate & conduct risk analysis
Review findings & decide Agency action
Issue Agency decision to Responsible Organization
SPII Incident?
NO
Yes
Notify US CERT
Investigate Incident
Develop findings issue report to BET
Review findings and issue recommendations to BET EX
BET EX Decide Agency action
Consensus?
Yes
No
Issue Agency decision to Responsible Organization
BNT decides Agency action
Issue Agency decision to Responsible Organization
RESPONSIBLE ORG. Implement agency decision
End
ROLES
Individual
EPA Call Center
CSIRC
Breach Evaluation Team Ex. Committee (BET EX)
Breach Evaluation Team (BET)
Responsible Organization
Breach Notification Team (BNT)